



Nessus – Ubuntu TargetJuice – Credentialled Scan

Report generated by Tenable Nessus™

Sun, 25 Jan 2026 00:18:15 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 172.16.135.130.....4

Vulnerabilities by Host

172.16.135.130



Scan Information

Start time: Sun Jan 25 00:05:56 2026
End time: Sun Jan 25 00:18:15 2026

Host Information

IP: 172.16.135.130
MAC Address: 00:0C:29:88:90:CF AE:ED:46:C2:40:CB 2A:BE:E2:2B:81:F4 A6:86:FD:D8:2D:74
OS: Linux Kernel 6.8.0-90-generic on Ubuntu 24.04

Vulnerabilities

260923 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : ImageMagick vulnerabilities (USN-7728-1)

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-7728-1 advisory.

It was discovered that ImageMagick did not properly process certain format strings when interpreting image filenames. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service. (CVE-2025-53014)

It was discovered that ImageMagick did not properly process certain format strings when interpreting image filenames. An attacker could possibly use this issue to cause ImageMagick to consume resources, resulting in a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 24.04 LTS. (CVE-2025-53019)

It was discovered that ImageMagick did not properly process certain format strings when interpreting image filenames. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-53101)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7728-1>

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

0.0004

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

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

STIG Severity

II

References

CVE	CVE-2025-53014
CVE	CVE-2025-53019
CVE	CVE-2025-53101
XREF	IAVB:2025-B-0117-S
XREF	USN:7728-1

Plugin Information

Published: 2025/09/03, Modified: 2025/09/03

Plugin Output

tcp/0

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

- Installed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm1
- Installed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm1
- Installed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm1
- Installed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm1

265697 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : ImageMagick vulnerabilities (USN-7756-1)

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-7756-1 advisory.

It was discovered that ImageMagick did not properly handle memory when performing magnified size calculations. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-55154)

Woojin Park, Hojun Lee, Youngin Won, and Siyeon Han discovered that ImageMagick incorrectly handled creating thumbnail images for certain dimensions. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service. This issue only affected Ubuntu 24.04 LTS.

(CVE-2025-55212)

Lumina Mescuwa discovered that ImageMagick did not properly handle cloning splay trees in the MagickCore library. An attacker could possibly use this issue to cause sanitized builds of ImageMagick to crash, resulting in a denial of service. (CVE-2025-55160)

Lumina Mescuwa discovered that ImageMagick did not properly handle memory. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-57807)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7756-1>

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

0.0004

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

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

STIG Severity

I

References

CVE	CVE-2025-55154
CVE	CVE-2025-55160
CVE	CVE-2025-55212
CVE	CVE-2025-57807
XREF	IAVB:2025-B-0145
XREF	USN:7756-1

Plugin Information

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

Plugin Output

tcp/0

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

- Installed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm2
- Installed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm2
- Installed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm2

```
- Installed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package    : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm2
```

269997 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : ImageMagick vulnerabilities (USN-7812-1)

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-7812-1 advisory.

Woojin Park, Hojun Lee, Yougin Won and Siyeon Han discovered that ImageMagick did not properly sanitize image file names. An attacker could possibly use this issue to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2025-55298)

Lumina Mescuwa discovered that ImageMagick did not properly handle memory when encoding BMP images. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-57803)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7812-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0016

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-2025-55298
CVE CVE-2025-57803
XREF USN:7812-1

Plugin Information

Published: 2025/10/10, Modified: 2025/10/10

Plugin Output

tcp/0

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

- Installed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm3
- Installed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm3
- Installed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm3
- Installed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm3

276520 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : ImageMagick vulnerabilities (USN-7876-1)

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-7876-1 advisory.

It was discovered that ImageMagick did not properly handle memory when encoding BMP images. An attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue exists due to an incomplete fix for CVE-2025-57803.

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

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

See Also

<https://ubuntu.com/security/notices/USN-7876-1>

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

0.0004

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-2025-62171
XREF IAVB:2025-B-0178
XREF USN:7876-1

Plugin Information

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

Plugin Output

tcp/0

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

```
- Installed package : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2build2
- Fixed package   : imagemagick-6-common_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm4

- Installed package : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2build2
- Fixed package   : libmagickcore-6.q16-7-extra_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm4

- Installed package : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package   : libmagickcore-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm4

- Installed package : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2build2
- Fixed package   : libmagickwand-6.q16-7t64_8:6.9.12.98+dfsg1-5.2ubuntu0.1~esm4
```

198152 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : FFmpeg vulnerabilities (USN-6803-1)

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-6803-1 advisory.

Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 24.04 LTS. (CVE-2023-49501)

Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-49502)

Zhang Ling and Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-49528)

Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-50007)

Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-50008)

Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10. (CVE-2023-50009)

Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-50010)

Zeng Yunxiang and Li Zeyuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-51793)

Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10.

(CVE-2023-51794, CVE-2023-51798)

Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10. (CVE-2023-51795, CVE-2023-51796)

It was discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2024-31578)

It was discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2024-31582)

It was discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10. (CVE-2024-31585)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6803-1>

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

0.0045

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

|

References

CVE	CVE-2023-49501
CVE	CVE-2023-49502
CVE	CVE-2023-49528
CVE	CVE-2023-50007
CVE	CVE-2023-50008
CVE	CVE-2023-50009
CVE	CVE-2023-50010
CVE	CVE-2023-51793
CVE	CVE-2023-51794
CVE	CVE-2023-51795
CVE	CVE-2023-51796
CVE	CVE-2023-51798
CVE	CVE-2024-31578
CVE	CVE-2024-31582
CVE	CVE-2024-31585
XREF	USN:6803-1
XREF	IAVB:2024-B-0041-S
XREF	IAVB:2024-B-0110-S

Plugin Information

Published: 2024/05/30, Modified: 2025/09/03

Plugin Output

tcp/0

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

- Installed package : libavcodec60_7:6.1.1-3ubuntu5
- Fixed package : libavcodec60_7:6.1.1-3ubuntu5+esml
- Installed package : libavfilter9_7:6.1.1-3ubuntu5
- Fixed package : libavfilter9_7:6.1.1-3ubuntu5+esml
- Installed package : libavformat60_7:6.1.1-3ubuntu5
- Fixed package : libavformat60_7:6.1.1-3ubuntu5+esml
- Installed package : libavutil58_7:6.1.1-3ubuntu5
- Fixed package : libavutil58_7:6.1.1-3ubuntu5+esml

```
- Installed package : libpostproc57_7:6.1.1-3ubuntu5
- Fixed package    : libpostproc57_7:6.1.1-3ubuntu5+esml

- Installed package : libswresample4_7:6.1.1-3ubuntu5
- Fixed package    : libswresample4_7:6.1.1-3ubuntu5+esml

- Installed package : libswscale7_7:6.1.1-3ubuntu5
- Fixed package    : libswscale7_7:6.1.1-3ubuntu5+esml
```

233301 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : zvbi vulnerabilities (USN-7367-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7367-1 advisory.

It was discovered that zvbi incorrectly handled memory when processing user input. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

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

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

See Also

<https://ubuntu.com/security/notices/USN-7367-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

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

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

VPR Score

3.6

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2025-2173
CVE	CVE-2025-2174
CVE	CVE-2025-2175
CVE	CVE-2025-2176
CVE	CVE-2025-2177
XREF	IAVA:2025-A-0190
XREF	USN:7367-1

Plugin Information

Published: 2025/03/24, Modified: 2025/03/24

Plugin Output

tcp/0

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

- Installed package : libzvbi-common_0.2.42-2
- Fixed package : libzvbi-common_0.2.42-2ubuntu0.24.04.1~esm1

- Installed package : libzvbi0t64_0.2.42-2
- Fixed package : libzvbi0t64_0.2.42-2ubuntu0.24.04.1~esm1

270676 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerabilities (USN-7823-1)

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 packages installed that are affected by multiple vulnerabilities as referenced in the USN-7823-1 advisory.

It was discovered that FFmpeg did not correctly handle certain memory operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 24.04 LTS. (CVE-2024-35365)

It was discovered that FFmpeg did not correctly handle certain integer calculations. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-35366)

It was discovered that FFmpeg may perform an out-of-bounds read under certain circumstances. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-35367)

It was discovered that FFmpeg did not correctly handle certain memory operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-35368)

It was discovered that FFmpeg did not correctly handle certain inputs, which could lead to an integer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-36613, CVE-2024-36616, CVE-2024-36618)

It was discovered that FFmpeg did not correctly handle certain inputs, which could lead to an integer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 24.04 LTS. (CVE-2024-36619)

It was discovered that FFmpeg did not correctly handle certain memory operations. A remote attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-7055)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7823-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0012

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-7055
CVE	CVE-2024-35365
CVE	CVE-2024-35366
CVE	CVE-2024-35367
CVE	CVE-2024-35368
CVE	CVE-2024-36613
CVE	CVE-2024-36616
CVE	CVE-2024-36618
CVE	CVE-2024-36619
XREF	IAVB:2024-B-0110-S
XREF	USN:7823-1

Plugin Information

Plugin Output

tcp/0

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

```
- Installed package : libavcodec60_7:6.1.1-3ubuntu5
- Fixed package   : libavcodec60_7:6.1.1-3ubuntu5+esm5

- Installed package : libavfilter9_7:6.1.1-3ubuntu5
- Fixed package   : libavfilter9_7:6.1.1-3ubuntu5+esm5

- Installed package : libavformat60_7:6.1.1-3ubuntu5
- Fixed package   : libavformat60_7:6.1.1-3ubuntu5+esm5

- Installed package : libavutil58_7:6.1.1-3ubuntu5
- Fixed package   : libavutil58_7:6.1.1-3ubuntu5+esm5

- Installed package : libpostproc57_7:6.1.1-3ubuntu5
- Fixed package   : libpostproc57_7:6.1.1-3ubuntu5+esm5

- Installed package : libswresample4_7:6.1.1-3ubuntu5
- Fixed package   : libswresample4_7:6.1.1-3ubuntu5+esm5

- Installed package : libswscale7_7:6.1.1-3ubuntu5
- Fixed package   : libswscale7_7:6.1.1-3ubuntu5+esm5
```

206422 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerability (USN-6983-1)

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-6983-1 advisory.

Zeng Yunxiang discovered that FFmpeg incorrectly handled memory during video encoding. An attacker could possibly use this issue to perform 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-6983-1>

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

0.0003

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-2024-32230

XREF USN:6983-1

XREF IAVB:2024-B-0110-S

Plugin Information

Published: 2024/09/02, Modified: 2025/02/13

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 : libavcodec60_7:6.1.1-3ubuntu5
- Fixed package : libavcodec60_7:6.1.1-3ubuntu5+esm2
- Installed package : libavfilter9_7:6.1.1-3ubuntu5
- Fixed package : libavfilter9_7:6.1.1-3ubuntu5+esm2
- Installed package : libavformat60_7:6.1.1-3ubuntu5
- Fixed package : libavformat60_7:6.1.1-3ubuntu5+esm2
- Installed package : libavutil58_7:6.1.1-3ubuntu5
- Fixed package : libavutil58_7:6.1.1-3ubuntu5+esm2
- Installed package : libpostproc57_7:6.1.1-3ubuntu5
- Fixed package : libpostproc57_7:6.1.1-3ubuntu5+esm2
- Installed package : libswresample4_7:6.1.1-3ubuntu5
- Fixed package : libswresample4_7:6.1.1-3ubuntu5+esm2
- Installed package : libswscale7_7:6.1.1-3ubuntu5
- Fixed package : libswscale7_7:6.1.1-3ubuntu5+esm2

271190 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerabilities (USN-7830-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7830-1 advisory.

It was discovered that FFmpeg incorrectly handled the return values of functions in its Firequalizer filter and in the HTTP Live Streaming (HLS) implementation, leading to a NULL pointer dereference. If a user was tricked into loading a crafted media file, a remote attacker could possibly use this issue to make FFmpeg crash, resulting in a denial of service. (CVE-2023-6603, CVE-2025-10256)

It was discovered that FFmpeg did not enforce an input format before triggering the HTTP demuxer. A remote attacker could possibly use this issue to perform a Server-Side Request Forgery (SSRF) attack. (CVE-2025-6605)

It was discovered that FFmpeg incorrectly handled memory allocation in the ALS audio decoder. If a user was tricked into loading a crafted media file, a remote attacker could possibly use this issue to make FFmpeg crash, resulting in a denial of service. (CVE-2025-7700)

It was discovered that FFmpeg incorrectly handled memory in the JPEG 2000 decoder, which could lead to a heap buffer overflow. If a user or application were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service or leak sensitive information. (CVE-2025-9951)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7830-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

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

5.9

EPSS Score

0.0027

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-6603
CVE	CVE-2023-6605
CVE	CVE-2025-7700
CVE	CVE-2025-9951
CVE	CVE-2025-10256
XREF	IAVB:2024-B-0110-S
XREF	IAVB:2025-B-0018-S
XREF	IAVB:2025-B-0150
XREF	USN:7830-1

Plugin Information

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

Plugin Output

tcp/0

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

- Installed package : libavcodec60_7:6.1.1-3ubuntu5
- Fixed package : libavcodec60_7:6.1.1-3ubuntu5+esm6
- Installed package : libavfilter9_7:6.1.1-3ubuntu5
- Fixed package : libavfilter9_7:6.1.1-3ubuntu5+esm6
- Installed package : libavformat60_7:6.1.1-3ubuntu5
- Fixed package : libavformat60_7:6.1.1-3ubuntu5+esm6
- Installed package : libavutil58_7:6.1.1-3ubuntu5
- Fixed package : libavutil58_7:6.1.1-3ubuntu5+esm6
- Installed package : libpostproc57_7:6.1.1-3ubuntu5
- Fixed package : libpostproc57_7:6.1.1-3ubuntu5+esm6
- Installed package : libswresample4_7:6.1.1-3ubuntu5
- Fixed package : libswresample4_7:6.1.1-3ubuntu5+esm6
- Installed package : libswscale7_7:6.1.1-3ubuntu5
- Fixed package : libswscale7_7:6.1.1-3ubuntu5+esm6

237868 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : GStreamer Bad Plugins vulnerabilities (USN-7558-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7558-1 advisory.

It was discovered that the AV1 codec plugin in GStreamer could be made to write out of bounds. An attacker could possibly use this issue to cause applications using the plugin to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2023-50186, CVE-2024-0444)

It was discovered that the H265 codec plugin in GStreamer could be made to write out of bounds. An attacker could possibly use this issue to cause applications using the plugin to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-3887)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7558-1>

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

6.7

EPSS Score

0.0147

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-2023-50186
CVE	CVE-2024-0444
CVE	CVE-2025-3887
XREF	USN:7558-1

Plugin Information

Published: 2025/06/05, Modified: 2025/06/05

Plugin Output

tcp/0

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

- Installed package : gstreamer1.0-plugins-bad_1.24.2-1ubuntu4
- Fixed package : gstreamer1.0-plugins-bad_1.24.2-1ubuntu4+esm1

- Installed package : libgstreamer-plugins-bad1.0-0_1.24.2-1ubuntu4
- Fixed package : libgstreamer-plugins-bad1.0-0_1.24.2-1ubuntu4+esm1

197836 - Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : cJSON vulnerabilities (USN-6784-1)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6784-1 advisory.

It was discovered that cJSON incorrectly handled certain input. An attacker could possibly use this issue to cause cJSON to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-50471, CVE-2023-50472)

Luo Jin discovered that cJSON incorrectly handled certain input. An attacker could possibly use this issue to cause cJSON to crash, resulting in a denial of service. (CVE-2024-31755)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6784-1>

Solution

Update the affected lib cJSON-dev and / or lib cJSON1 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

5.5

EPSS Score

0.0062

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-2023-50471
CVE	CVE-2023-50472
CVE	CVE-2024-31755
XREF	USN:6784-1

Plugin Information

Published: 2024/05/23, Modified: 2025/09/03

Plugin Output

tcp/0

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

- Installed package : libcjson1_1.7.17-1
- Fixed package : libcjson1_1.7.17-1ubuntu0.1~esm2

234475 - Ubuntu 22.04 LTS / 24.04 LTS : 7-Zip vulnerabilities (USN-7438-1)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7438-1 advisory.

Igor Pavlov discovered that 7-Zip had several memory-related issues. An attacker could possibly use these issues to cause 7-Zip to crash, resulting in a denial of service, or execute arbitrary code.

(CVE-2023-52168, CVE-2023-52169)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7438-1>

Solution

Update the affected 7zip and / or 7zip-standalone packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0039

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2023-52168
CVE CVE-2023-52169
XREF IAVA:2024-A-0765-S
XREF USN:7438-1

Plugin Information

Published: 2025/04/16, Modified: 2025/04/16

Plugin Output

tcp/0

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

- Installed package : 7zip_23.01+dfsg-11
- Fixed package : 7zip_23.01+dfsg-11ubuntu0.1~esml

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

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 v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :
```

```
| -Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=dba8ef2bf78c
| -Issuer   : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
|           Certification Authority
```

237485 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : FFmpeg vulnerabilities (USN-7538-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7538-1 advisory.

Simcha Kosman discovered that FFmpeg did not correctly handle certain return values. An attacker could possibly use this issue to leak sensitive information. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS and Ubuntu 24.10. (CVE-2025-0518)

It was discovered that FFmpeg did not correctly handle certain memory operations. A remote attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 24.10. (CVE-2025-1816)

It was discovered that FFmpeg contained a reachable assertion, which could lead to a failure when processing certain AAC files. If a user or automated system were tricked into opening a specially crafted AAC file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS and Ubuntu 24.10.

(CVE-2025-22919)

It was discovered that FFmpeg did not correctly handle certain memory operations. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, Ubuntu 24.10 and Ubuntu 25.04. (CVE-2025-22921)

It was discovered that FFmpeg did not correctly handle certain memory operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 24.04 LTS, Ubuntu 24.10 and Ubuntu 25.04. (CVE-2025-25473)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7538-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.001

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

II

References

CVE	CVE-2025-0518
CVE	CVE-2025-1816
CVE	CVE-2025-22919
CVE	CVE-2025-22921
CVE	CVE-2025-25473
XREF	IAVB:2025-B-0018-S
XREF	USN:7538-1

Plugin Information

Published: 2025/05/29, Modified: 2025/05/29

Plugin Output

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

- Installed package : libavcodec60_7:6.1.1-3ubuntu5
- Fixed package : libavcodec60_7:6.1.1-3ubuntu5+esm3
- Installed package : libavfilter9_7:6.1.1-3ubuntu5
- Fixed package : libavfilter9_7:6.1.1-3ubuntu5+esm3
- Installed package : libavformat60_7:6.1.1-3ubuntu5
- Fixed package : libavformat60_7:6.1.1-3ubuntu5+esm3
- Installed package : libavutil58_7:6.1.1-3ubuntu5
- Fixed package : libavutil58_7:6.1.1-3ubuntu5+esm3
- Installed package : libpostproc57_7:6.1.1-3ubuntu5
- Fixed package : libpostproc57_7:6.1.1-3ubuntu5+esm3
- Installed package : libswresample4_7:6.1.1-3ubuntu5
- Fixed package : libswresample4_7:6.1.1-3ubuntu5+esm3
- Installed package : libswscale7_7:6.1.1-3ubuntu5
- Fixed package : libswscale7_7:6.1.1-3ubuntu5+esm3

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

2.2

EPSS Score

0.0037

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0524

XREF CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The remote clock is synchronized with the local clock.

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : 1
Vendor       : VMware, Inc.
Release Date : 07/21/2025
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/09/29

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :  
cpe:/o:canonical:ubuntu_linux:24.04.3:~~lts~~~ -> Canonical Ubuntu Linux  
  
Following application CPE's matched on the remote system :  
cpe:/a:docker:docker:28.2.2 -> Docker  
cpe:/a:exiv2:libexiv2:0.27.6  
cpe:/a:gnupg:libgcrypt:1.10.3 -> GnuPG Libgcrypt  
cpe:/a:haxx:curl:8.5.0 -> Haxx Curl  
cpe:/a:haxx:libcurl:8.5.0 -> Haxx libcurl  
cpe:/a:igor_sysoev:nginx:1.24.0 -> Nginx  
cpe:/a:linuxfoundation:containerd:1.7.28 -> The Linux Foundation containerd  
cpe:/a:nginx:nginx:1.24.0 -> Nginx  
cpe:/a:nginx:nginx:1.24.0-2 -> Nginx  
cpe:/a:openbsd:openssh:9.6 -> OpenBSD OpenSSH  
cpe:/a:openbsd:openssl:9.6p1 -> OpenBSD OpenSSH  
cpe:/a:openssl:openssl:3.0.13 -> OpenSSL Project OpenSSL
```

```
cpe:/a:smartbedded:meteobridge_firmware  
cpe:/a:tenable:nessus -> Tenable Nessus  
cpe:/a:tukaani:xz:5.6.1 -> Tukaani XZ  
cpe:/a:vim:vim:9.1 -> Vim  
cpe:/a:vmware:open_vm_tools:12.5.0 -> VMware Open VM Tools  
x-cpe:/a:libndp:libndp:1.8
```

237414 - Containerd Installed (Linux)

Synopsis

containerd was detected on the remote host.

Description

containerd, a container runtime which can manage the complete container lifecycle of its host system is installed on the target host.

See Also

<https://github.com/containerd/containerd/tree/main>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/28, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path          : /usr/bin/containerd
Version       : 1.7.28
Associated Package : containerd 1.7.28-0ubuntu1
Managed by OS    : True
```

182774 - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.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: 2023/10/09, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path          : /usr/bin/curl
Version      : 8.5.0
Associated Package : curl 8.5.0-2ubuntu10.6
Managed by OS    : True
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/12/15

Plugin Output

tcp/0

```
Hostname : targetjuice
targetjuice (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

159488 - Docker Installed (Linux)

Synopsis

Docker was detected on the remote host.

Description

A container virtualization suite is installed on the remote host.

See Also

<https://www.docker.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/04/04, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path      : /usr/bin/docker
Version   : 28.2.2
Build     : 28
Managed by OS : True
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/09/24

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :
```

- 172.18.0.1 (on interface br-e70f8e9f057e)
- 172.17.0.1 (on interface docker0)
- 172.16.135.130 (on interface enp2s0)
- 127.0.0.1 (on interface lo)

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/09/24

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :
```

- fe80::28be:e2ff:fe2b:81f4 (on interface br-e70f8e9f057e)
- fe80::a486:fdff:fed8:2d74 (on interface docker0)
- fe80::20c:29ff:fe88:90cf (on interface enp2s0)
- ::1 (on interface lo)
- fe80::aced:46ff:fec2:40cb (on interface veth5eaf836)

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

```
The following MAC addresses exist on the remote host :
```

- 00:0c:29:88:90:cf (interface enp2s0)
- ae:ed:46:c2:40:cb (interface veth5eaf836)
- 2a:be:e2:2b:81:f4 (interface br-e70f8e9f057e)
- a6:86:fd:d8:2d:74 (interface docker0)

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
veth5eaf836:  
  MAC : ae:ed:46:c2:40:cb  
  IPv6:  
    - Address : fe80::aced:46ff:fed2:40cb  
      Prefixlen : 64  
      Scope : link  
      ScopeID : 0x20  
  lo:  
  IPv4:  
    - Address : 127.0.0.1  
      Netmask : 255.0.0.0  
  IPv6:  
    - Address : ::1  
      Prefixlen : 128  
      Scope : host  
      ScopeID : 0x10  
docker0:  
  MAC : a6:86:fd:d8:2d:74  
  IPv4:  
    - Address : 172.17.0.1  
      Netmask : 255.255.0.0  
      Broadcast : 172.17.255.255  
  IPv6:  
    - Address : fe80::a486:fdff:fed8:2d74  
      Prefixlen : 64  
      Scope : link  
      ScopeID : 0x20  
enp2s0:  
  MAC : 00:0c:29:88:90:cf  
  IPv4:  
    - Address : 172.16.135.130  
      Netmask : 255.255.255.0
```

```
        Broadcast : 172.16.135.255
IPv6:
- Address : fe80::20c:29ff:fe88:90cf
  Prefixlen : 64
  Scope : link
  ScopeID : 0x20
br-e70f8e9f057e:
MAC : 2a:be:e2:2b:81:f4
IPv4:
- Address : 172.18.0.1
  Netmask : 255.255.0.0
  Broadcast : 172.18.255.255
IPv6:
- Address : fe80::28be:e2ff:fe2b:81f4
  Prefixlen : 64
  Scope : link
  ScopeID : 0x20
```

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:  
  enp2s0:  
    ipv4_gateways:  
      172.16.135.2:  
        subnets:  
          - 0.0.0.0/0  
Interface Routes:  
  br-e70f8e9f057e:  
    ipv4_subnets:  
      - 172.18.0.0/16  
    ipv6_subnets:  
      - fe80::/64  
  docker0:  
    ipv4_subnets:  
      - 172.17.0.0/16  
    ipv6_subnets:  
      - fe80::/64  
  enp2s0:  
    ipv4_subnets:  
      - 172.16.135.0/24  
    ipv6_subnets:  
      - fe80::/64  
  veth5eaf836:  
    ipv6_subnets:  
      - fe80::/64
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :
```

```
/usr/local/sbin
/usr/local/bin
/usr/sbin
/usr/bin
/sbin
/bin
/usr/games
/usr/local/games
/snap/bin
```

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:29:88:90:CF : 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: 2025/06/10

Plugin Output

tcp/0

The following is a consolidated list of detected MAC addresses:

- 00:0C:29:88:90:CF
- AE:ED:46:C2:40:CB
- 2A:BE:E2:2B:81:F4
- A6:86:FD:D8:2D:74

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :
```

```
nginx/1.24.0 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8834/www

```
The remote web server type is :
```

```
NessusWWW
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Server: nginx/1.24.0 (Ubuntu)
Date: Sun, 25 Jan 2026 05:06:25 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Tue, 13 Jan 2026 03:56:50 GMT
Connection: keep-alive
ETag: "6965c282-267"
Accept-Ranges: bytes

Response Body :

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
```

```
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Cache-Control: must-revalidate
X-Frame-Options: DENY
Content-Type: text/html
ETag: 6bla219f17643a61ccea77e06731338e
Connection: close
X-XSS-Protection: 1; mode=block
Server: NessusWWW
Date: Sun, 25 Jan 2026 05:06:25 GMT
X-Content-Type-Options: nosniff
Content-Length: 1629
Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action
'self'; frame-ancestors 'none'; frame-src https://store.tenable.com www.youtube.com; default-src
'self'; connect-src 'self' datanessus-telemetry.tenable.com contentnessus-telemetry.tenable.com
api.tenable.com www.tenable.com; script-src 'self' contentnessus-telemetry.tenable.com
www.tenable.com; img-src 'self' datacontentnessus-telemetry.tenable.com data.nessus-
telemetry.tenable.com pendo-static-5689996938182656.storage.googleapis.com s.ytimg.com i.ytimg.com;
```

```
style-src 'self' content.nessus-telemetry.tenable.com data.nessus-telemetry.tenable.com pendo-
static-5689996938182656.storage.googleapis.com www.tenable.com; object-src 'none'; base-uri 'self';
Strict-Transport-Security: max-age=31536000; includeSubDomains
Expect-CT: max-age=0
```

Response Body :

```
<!doctype html>
<html lang="en">
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com www.youtube.com; default-src
'self'; connect-src 'self' data.nessus-telemetry.tenable.com content.nessus-telemetry.tenable.com
api.tenable.com www.tenable.com; script-src 'self' content.nessus-telemetry.tenable.com
www.tenable.com; img-src 'self' data: data.nessus-telemetry.tenable.com content.nessus-
telemetry.tenable.com pendo-static-5689996938182656.storage.googleapis.com s.ytimg.com i.ytimg.com;
style-src 'self' c [...]
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/12/15

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address      : 127.0.0.1
  Assign Method : static
+ IPv6
- Address      : ::1
  Assign Method : static
+ enp2s0
+ IPv4
- Address      : 172.16.135.130
  Assign Method : dynamic
+ IPv6
- Address      : fe80::20c:29ff:fe88:90cf
  Assign Method : static
+ docker0
+ IPv4
- Address      : 172.17.0.1
  Assign Method : static
+ IPv6
- Address      : fe80::a486:fdff:fed8:2d74
  Assign Method : static
+ br-e70f8e9f057e
+ IPv4
- Address      : 172.18.0.1
  Assign Method : static
+ IPv6
- Address      : fe80::28be:e2ff:fe2b:81f4
  Assign Method : static
+ veth5eaf836@if2
+ IPv6
- Address      : fe80::aced:46ff:fec2:40cb
```

Assign Method : static

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

<https://gnupg.org/download/index.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:  
Path      : /usr/lib/aarch64-linux-gnu/libgcrypt.so.20.4.3  
Version   : 1.10.3  
  
Path      : /usr/lib/aarch64-linux-gnu/libgcrypt.so.20  
Version   : 1.10.3  
  
Path      : /lib/aarch64-linux-gnu/libgcrypt.so.20.4.3  
Version   : 1.10.3  
  
Path      : /lib/aarch64-linux-gnu/libgcrypt.so.20  
Version   : 1.10.3
```

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.200214' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://github.com/jpirko/libndp>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path      : libndp0 1.8-1fakesyncubuntu0.24.04.1 (via package manager)
Version   : 1.8
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
tmpfs                 391M  1.7M  389M   1% /run
efivars                256K   34K  223K  14% /sys/firmware/efi/efivars
/dev/mapper/ubuntu--vg-ubuntu--lv    62G   19G   40G  32% /
tmpfs                  2.0G     0   2.0G   0% /dev/shm
tmpfs                  5.0M   8.0K   5.0M   1% /run/lock
/dev/nvme0n1p2          1.7G  205M   1.4G  13% /boot
/dev/nvme0n1p1          952M  6.4M  945M   1% /boot/efi
tmpfs                 391M  144K  391M   1% /run/user/1000

$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0      7:0    0 68.9M  1 loop /snap/core22/2194
loop1      7:1    0   4K  1 loop /snap/bare/5
loop2      7:2    0 68.9M  1 loop /snap/core22/2218
loop3      7:3    0 493.6M 1 loop /snap/gnome-42-2204/228
loop4      7:4    0 236.1M 1 loop /snap/firefox/7631
loop5      7:5    0 236.1M 1 loop /snap/firefox/7669
loop6      7:6    0  503M 1 loop /snap/gnome-42-2204/245
loop7      7:7    0  91.7M 1 loop /snap/gtk-common-themes/1535
loop8      7:8    0  44.3M 1 loop /snap/snapd/25585
loop9      7:9    0  41.6M 1 loop /snap/snapd/25939
loop10     7:10   0 219.4M 1 loop /snap/thunderbird/918
```

```
loop11          7:11    0 219.2M  1 loop  /snap/thunderbird/934
sr0            11:0    1 1024M  0 rom
nvme0n1        259:0    0   65G  0 disk
##nvme0n1p1    259:1    0   953M  0 part  /boot/efi
##nvme0n1p2    259:2    0   1.8G  0 part  /boot
##nvme0n1p3    259:3    0   62.3G 0 part
##ubuntu--vg-ubuntu--lv 252:0    0   62.3G 0 lvm   /
```

```
$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev  [...]
```

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: UTC +0000
Via timedatectl: Time zone: Etc/UTC (UTC, +0000)
Via /etc/timezone: Etc/UTC
Via /etc/localtime: UTC0
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

```
-----[ User Accounts ]-----
User      : cyberic
Home folder  : /home/cyberic
Start script : /bin/bash
Groups      : lxd
              cdrom
              cyberic
              docker
              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 : /run/ircd
Start script: /usr/sbin/nologin
Groups      : irc

User        : _apt
Home folder : /nonexistent
Start script: /usr/sbin/nologin

```

```
Groups      : nogroup
User       : nobody
Home folder : [...]
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 10.11.1  
Nessus build : 20021  
Plugin feed version : 202512261655  
Scanner edition used : Nessus Home  
Scanner OS : LINUX  
Scanner distribution : ubuntu1804-aarch64  
Scan type : Normal  
Scan name : Nessus - Ubuntu TargetJuice - Credentialed Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 172.17.0.2
Port scanner(s) : netstat
Port range : default
Ping RTT : 8.473 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'cyberic' 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 : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/1/25 0:06 EST (UTC -05:00)
Scan duration : 727 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

<https://www.tenable.com/products/nessus/nessus-professional>

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2025/11/03

Plugin Output

tcp/8834/www

```
URL      : https://172.16.135.130:8834/
Version  : unknown
```

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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

udp/5353

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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

tcp/8834/www

Port 8834/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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

udp/34848

```
Port 34848/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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

udp/49054

```
Port 49054/udp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Cisco HyperFlex 5
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 6.8.0-90-generic
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux targetjuice 6.8.0-90-generic #91-Ubuntu SMP PREEMPT_DYNAMIC Tue Nov 18
13:53:54 UTC 2025 aarch64 aarch64 aarch64 GNU/Linux

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W64240:00204ffff:M1460:
P2:B10113:F0x12:W65160:00204ffff0402080afffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191601_7_p=22R

Remote operating system : Linux Kernel 6.8.0-90-generic on Ubuntu 24.04
Confidence level : 100
```

```
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
  SSH:!::SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14
HTTP:!::Server: nginx/1.24.0 (Ubuntu)

SSLcert:!::i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
Authorities/CN:dba8ef2bf78cs/O:Nessus Users Uniteds/OU:Nessus Server
6029d9cca67f39cf8e9ef2f66c290d4816fc2b01
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.8.0-90-generic on Ubuntu 24.04
Confidence level : 100
Method : LinuxDistribution
```

```
The remote host is running Linux Kernel 6.8.0-90-generic on Ubuntu 24.04
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux targetjuice 6.8.0-90-generic #91-Ubuntu SMP PREEMPT_DYNAMIC Tue Nov 18 13:53:54 UTC 2025
aarch64 aarch64 aarch64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
trixie/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 4.857132 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  : cyberic
Protocol : SSH
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/12/15

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 9.6p1
Banner  : SSH-2.0-OpenSSH_9.6p1_Ubuntu-3ubuntu13.14
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 2 installs of OpenSSL:

Path          : /usr/lib/aarch64-linux-gnu/libcrypto.so.3
Version       : 3.0.13
Associated Package : libssl13t64

Path          : /usr/bin/openssl
Version       : 3.0.13
Associated Package : openssl 3.0.13-0ubuntu3.6
Managed by OS   : True
```

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/aarch64-linux-gnu/libssl.so.3

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

Successfully retrieved and stored package data.

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/12/15

Plugin Output

tcp/0

```
. You need to take the following 7 actions :

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : ImageMagick
vulnerabilities (USN-7876-1) (276520) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : FFmpeg
vulnerabilities (USN-7538-1) (237485) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : zvbi vulnerabilities
(USN-7367-1) (233301) ]

+ Action to take : Update the affected packages.
```

```
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerabilities (USN-7830-1) (271190) ]
```

```
+ Action to take : Update the affected packages.
```

```
+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : GStreamer Bad Plugins vulnerabilities (USN-7558-1) (237868) ]
```

```
+ Action to take : Update the affected packages.
```

```
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : cJSON vulnerabilities (USN-6784-1) (197836) ]
```

```
+ Action to take : Update the affected lib cJSON-dev and / or lib cJSON1 packages.
```

```
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 22.04 LTS / 24.04 LTS : 7-Zip vulnerabilities (USN-7438-1) (234475) ]
```

```
+ Action to take : Update the affected 7zip and / or 7zip-standalone packages.
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.

However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

<http://www.nessus.org/u?7a390f87>
<http://www.nessus.org/u?ad7d6b3b>
<http://www.nessus.org/u?1c0c61e0>
<http://www.nessus.org/u?5eec4b28>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/22/ssh

The target SSH server offers no post-quantum ciphers.

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.

However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

<http://www.nessus.org/u?7a390f87>

<http://www.nessus.org/u?ad7d6b3b>

<http://www.nessus.org/u?1c0c61e0>

<http://www.nessus.org/u?5eec4b28>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/8834/www

The target TLS server offers no post-quantum ciphers.

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/12/08

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :  
  
Client to Server: aes256-ctr  
Server to Client: aes256-ctr  
  
The server supports the following options for compression_algorithms_server_to_client :  
  
none  
zlib@openssh.com  
  
The server supports the following options for mac_algorithms_client_to_server :  
  
hmac-sha1  
hmac-sha1-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com  
umac-64-etm@openssh.com  
umac-64@openssh.com  
  
The server supports the following options for server_host_key_algorithms :  
  
ecdsa-sha2-nistp256  
rsa-sha2-256  
rsa-sha2-512  
ssh-ed25519
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr  
aes128-gcm@openssh.com  
aes192-ctr  
aes256-ctr  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

```
The server supports the following options for mac_algorithms_server_to_client :
```

```
hmac-sha1  
hmac-sha1-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com  
umac-64-etm@openssh.com  
umac-64@openssh.com
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256  
curve25519-sha256@libssh.org  
diffie-hellman-group-exchange-sha256  
diffie-hellman-group14-sha256  
diffie-hellman-group16-sha512  
diffie-hellman-group18-sha512  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521  
ext-info-s  
kex-strict-s-v00@openssh.com  
sntrup761x25519-sha512@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 encryption_algorithms_server_to_client :
```

```
aes128-ctr  
aes128-gcm@openssh.com  
aes192-ctr  
aes256-ctr  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : cyberic
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 3.5\n# No SMBIOS nor DMI entry point found, sorry."
        Error       : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied"
      - Command      : "LC_ALL=C /usr/sbin/dmidecode"
        Response    : "# dmidecode 3.5\n# No SMBIOS nor DMI entry point found, sorry."
        Error       : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied"
      - Command      : "LC_ALL=C /sbin/dmidecode"
        Response    : "# dmidecode 3.5\n# No SMBIOS nor DMI entry point found, sorry."
```

```
    Error      : "\n/sys/firmware/dmi/tables/smbios_entry_point: 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"
  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"
  Error          : ""
- Command       : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
  Response        : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied"
  Error          : ""
- Command       : "LC_ALL=C /sbin/dmidecode -s chassis-asset-tag 2>&1"
  Response        : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied"
  Error          : ""
- Plugin Filename : linux_kernel_speculative_execution_detect.nbin
  Plugin ID       : 125216
  Plugin Name     : Processor Speculative Execution [...]
```

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
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
    hmac-sha1
```

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_9.6p1 Ubuntu-3ubuntu13.14
SSH supported authentication : publickey,password
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/8834/www

This port supports TLSv1.3/TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

```
Subject Name:  
  
Organization: Nessus Users United  
Organization Unit: Nessus Server  
Locality: New York  
Country: US  
State/Province: NY  
Common Name: dba8ef2bf78c  
  
Issuer Name:  
  
Organization: Nessus Users United  
Organization Unit: Nessus Certification Authority  
Locality: New York  
Country: US  
State/Province: NY  
Common Name: Nessus Certification Authority  
  
Serial Number: 00 82 2D  
  
Version: 3  
  
Signature Algorithm: SHA-256 With RSA Encryption  
  
Not Valid Before: Jan 25 04:05:17 2026 GMT  
Not Valid After: Jan 24 04:05:17 2030 GMT  
  
Public Key Info:  
  
Algorithm: RSA Encryption  
Key Length: 2048 bits  
Public Key: 00 9A AC 3D FE C2 C2 F6 17 DA DD D2 4F F8 FA A6 4D 39 6D E0
```

```
E6 B6 D9 7D 24 78 C9 F0 21 1E AD 59 4B 36 73 18 E3 08 16 AB
C0 7F 4C 5F ED 90 85 6F 62 D8 83 39 57 1A DA 6D 93 EB 02 19
20 56 8E DE 51 15 5D 6F D3 20 9F 56 EE 8A A8 A3 F1 C0 06 0E
07 7E B4 A6 EE D6 A9 01 5F 06 36 93 CF 7E 06 1E AD 24 E0 35
A1 FF 73 D1 93 4B 4F 4B BC B9 56 FE C4 09 E8 84 91 13 E3 DA
64 7F 4C F1 A3 7A E4 A3 68 EE 19 AB 4C 4F 20 56 25 5D DA E1
33 ED 3E 79 8D AA 0A 96 8B BE BC 5C 78 B6 83 8C BE 02 03 C1
54 83 FC 1E E8 F0 A2 8E AE D5 1F B5 C2 97 D1 D6 24 13 2E 9A
3D 8E B1 57 6B 77 6F 4A B3 51 65 29 DE F5 D3 11 68 90 45 AF
48 FF 54 1D 6F D0 FC 26 0C 47 AC D5 37 69 4E 53 11 50 2F B7
34 B1 9D 6B 2E 7B F4 49 55 D8 5D E8 07 DD 4C 31 E4 12 16 82
19 75 0E FD 49 9D 30 41 AF E3 BF 0C 57 31 5E 00 29
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

```
Signature: 00 65 90 68 1C A2 4D 49 3C CB 4E ED DE 55 F2 28 7B BE B0 55
38 A8 2D 8E D5 65 C2 BB 08 2B 7B D1 79 A4 F3 F5 CB 8F B1 AE
26 30 CF 08 34 1F 3C 5B 39 51 48 F3 F4 50 1C C8 92 66 E4 B0
97 09 1C 46 8C 08 9E 97 A7 AE 61 BB 02 E4 93 AB 60 B0 1D 93
96 53 EF 2D E6 DD 73 23 DE 8E 91 DC A9 3D 36 45 FA A5 F6 5C
AB 64 B6 C4 FF C1 78 F6 94 CC DE D2 90 A2 1C D6 C1 F4 B5 B1
A1 EE 9C 2 [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>

<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8834/www

```
Here is the list of SSL ciphers supported by the remote server :  
Each group is reported per SSL Version.
```

```
SSL Version : TLSv13
```

```
High Strength Ciphers (>= 112-bit key)
```

Name	Code	KEX	Auth	Encryption	MAC
TLS_AES_256_GCM_SHA384 SHA384	0x13, 0x02	-	-	AES-GCM(256)	

```
SSL Version : TLSv12
```

```
High Strength Ciphers (>= 112-bit key)
```

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDHE	RSA	AES-GCM(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDHE	RSA	AES-GCM(256)	

```
The fields above are :
```

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8834/www

```
Here is the list of SSL PFS ciphers supported by the remote server :
```

```
High Strength Ciphers (>= 112-bit key)
```

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDHE	RSA	AES-GCM(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDHE	RSA	AES-GCM(256)	

```
The fields above are :
```

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}
```

```
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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: 2025/12/08

Plugin Output

tcp/22/ssh

An SSH server is running on this port.

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/80/www

A web server is running on this port.

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/8834/www

A TLSv1.3 server answered on this port.

tcp/8834/www

A web server is running on this port through TLSv1.3.

278501 - Smartbedded Meteobridge Web Detection

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM

<http://www.nessus.org/u?5ceb65be>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2025/12/15

Plugin Output

tcp/80/www

```
URL          : http://172.16.135.130/cgi-bin/meteobridge
Version      : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM

<http://www.nessus.org/u?5ceb65be>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2025/12/15

Plugin Output

tcp/8834/www

```
URL      : https://172.16.135.130:8834/cgi-bin/meteobridge
Version  : unknown
Authenticated : False
```

22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system : 

ii  7zip 23.01+dfsg-11 arm64 7-Zip file archiver with a high compression ratio
ii  accountsservice 23.13.9-2ubuntu6 arm64 query and manipulate user account information
ii  accountsservice-ubuntu-schemas 0.0.7+21.10.20210712-0ubuntu3 all AccountsService schemas
for Ubuntu
ii  acl 2.3.2-1build1.1 arm64 access control list - utilities
ii  activity-log-manager 0.9.7-0ubuntu31 arm64 blacklist configuration user interface for
Zeitgeist
ii  adduser 3.137ubuntu1 all add and remove users and groups
ii  adwaita-icon-theme 46.0-1 all default icon theme of GNOME
ii  alsa-base 1.0.25+dfsg-0ubuntu7 all ALSA driver configuration files
ii  alsa-topology-conf 1.2.5.1-2 all ALSA topology configuration files
ii  alsa-ucm-conf 1.2.10-1ubuntu5.8 all ALSA Use Case Manager configuration files
ii  alsaview 1.2.9-1ubuntu5 arm64 Utilities for configuring and using ALSA
ii  anacron 2.3-39ubuntu2 arm64 cron-like program that doesn't go by time
ii  apg 2.2.3.dfsg.1-5build3 arm64 Automated Password Generator - Standalone version
ii  apparmor 4.0.1really4.0.1-0ubuntu0.24.04.5 arm64 user-space parser utility for AppArmor
ii  apport 2.28.1-0ubuntu3.8 all automatically generate crash reports for debugging
ii  apport-core-dump-handler 2.28.1-0ubuntu3.8 all Kernel core dump handler for Apport
ii  apport-gtk 2.28.1-0ubuntu3.8 all GTK+ frontend for the apport crash report system
ii  apport-symptoms 0.25 all symptom scripts for apport
```

```
ii  appstream 1.0.2-1build6 arm64 Software component metadata management
ii  apt 2.8.3 arm64 commandline package manager
ii  apt-config-icons 1.0.2-1build6 all APT configuration snippet to enable icon downloads
ii  apt-config-icons-hidpi 1.0.2-1build6 all APT configuration snippet to enable HiDPI icon
downloads
ii  apt-utils 2.8.3 arm64 package management related utility programs
ii  aptdaemon 1.1.1+bzr98 [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

<http://www.nessus.org/u?2fb3aca6>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :  
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

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

277654 - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/10

Plugin Output

tcp/8834/www

```
These are the TLS supported groups offered by the remote server :
```

```
TLS supported groups :
```

Name	Code
<hr/>	
x25519	0x001d
secp256r1	0x0017
x448	0x001e
secp521r1	0x0019
secp384r1	0x0018
ffdhe2048	0x0100
ffdhe3072	0x0101
ffdhe4096	0x0102
ffdhe6144	0x0103
ffdhe8192	0x0104

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialled checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential  
did not have sufficient privileges for all planned checks :
```

```
User:      'cyberic'  
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:      'cyberic'
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 6.8.0-90-generic Fri Jan 23 01:16  still running
reboot    system boot 6.8.0-90-generic Mon Jan 12 15:22 - 07:11 (10+15:48)
reboot    system boot 6.8.0-71-generic Sun Jan 11 17:58 - 15:22 (21:24)
reboot    system boot 6.8.0-71-generic Thu Jan  8 20:09 - 02:09 (06:00)
reboot    system boot 6.8.0-71-generic Thu Jan  8 22:54 - 01:43 (02:49)
reboot    system boot 6.8.0-71-generic Thu Jan  8 22:24 - 22:54 (00:29)
reboot    system boot 6.8.0-71-generic Thu Jan  8 16:18 - 22:24 (06:06)
reboot    system boot 6.8.0-71-generic Thu Jan  8 18:21 - 22:16 (03:54)
reboot    system boot 6.8.0-71-generic Thu Jan  8 12:18 - 18:21 (06:02)
reboot    system boot 6.8.0-71-generic Wed Jan  7 22:50 - 18:16 (19:25)

wtmp begins Wed Jan  7 22:50:35 2026
```

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 172.17.0.2 to 172.16.135.130 :  
172.17.0.2  
172.16.135.130
```

```
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.192709' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://xz.tukaani.org/xz-utils/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:  
Path : /usr/lib/aarch64-linux-gnu/liblzma.so.5.4.5  
Version : 5.6.1  
Associated Package : liblzma5 5.6.1  
Confidence : High
```

```
Managed by OS      : True
Version Source    : Package

Path              : /usr/bin/xz
Version          : 5.6.1
Associated Package: xz-utils 5.6.1
Confidence       : High
Managed by OS      : True
Version Source    : Package
```

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	:	36ubuntu0~24.04

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	0.0	0.2	22932	11428	?	Ss	Jan24	0:11	/sbin/init
root	2	0.0	0.0	0	0	?	S	Jan24	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	Jan24	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/R-rcu_g]
root	5	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/R-rcu_p]
root	6	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/R-slub_]
root	7	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/R-netns]
root	10	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/0:0H-events_highpri]
root	12	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/R-mm_pe]
root	13	0.0	0.0	0	0	?	I	Jan24	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	Jan24	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	Jan24	0:00	[rcu_tasks_trace_kthread]
root	16	0.0	0.0	0	0	?	S	Jan24	0:06	[ksoftirqd/0]
root	17	0.0	0.0	0	0	?	I	Jan24	0:20	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	Jan24	0:00	[migration/0]
root	19	0.0	0.0	0	0	?	S	Jan24	0:00	[idle_inject/0]
root	20	0.0	0.0	0	0	?	S	Jan24	0:00	[cpuhp/0]
root	21	0.0	0.0	0	0	?	S	Jan24	0:00	[cpuhp/1]
root	22	0.0	0.0	0	0	?	S	Jan24	0:00	[idle_inject/1]
root	23	0.0	0.0	0	0	?	S	Jan24	0:00	[migration/1]
root	24	0.0	0.0	0	0	?	S	Jan24	0:03	[ksoftirqd/1]
root	26	0.0	0.0	0	0	?	I<	Jan24	0:00	[kworker/1:0H-events_highpri]
root	27	0.0	0.0	0	0	?	S	Jan24	0:00	[kdevtmpfs]
root	28	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 : cyberic  
Protocol : SSH
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

<https://kb.vmware.com/s/article/340>

<http://www.nessus.org/u?c0628155>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path      : /usr/bin/vmtoolsd
Version  : 12.5.0
```

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: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:  
Path      : /usr/bin/vim.tiny  
Version   : 9.1  
  
Path      : /usr/bin/vim.basic  
Version   : 9.1
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:  
Path : /usr/lib/aarch64-linux-gnu/libcurl.so.4.8.0  
Version : 8.5.0  
Associated Package : libcurl4t64  
  
Path : /usr/lib/aarch64-linux-gnu/libcurl-gnutls.so.4.8.0  
Version : 8.5.0  
Associated Package : libcurl3t64-gnutls
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://exiv2.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/12/18

Plugin Output

tcp/0

```
Path          : /usr/lib/aarch64-linux-gnu/libexiv2.so.0.27.6
Version      : 0.27.6
Associated Package : libexiv2-27 0.27.6-1build1
Managed by OS    : True
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL      : http://172.16.135.130/
Version  : 1.24.0
os       : Ubuntu
source   : Server: nginx/1.24.0 (Ubuntu)
```

136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

<https://www.nginx.com>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2025/12/18

Plugin Output

tcp/0

```
Nessus detected 2 installs of nginx:

Path      : nginx (via package manager)
Version   : 1.24.0-2

Path          : /usr/sbin/nginx
Version       : 1.24.0
Associated Package : nginx: /usr/sbin/nginx
Detection Method   : Running Process
Full Version     : 1.24.0
Managed by OS    : True
Nginx Plus      : False
```