Bsides-Vancouver-2018

Report generated by Tenable Nessus™ Wed, 29 Oct 2025 10:46:12 CET

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.50.3..... 4

Vulnerabilities by Host

192.168.50.3

13	25	28	7	84
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Oct 29 10:28:11 2025
End time: Wed Oct 29 10:46:11 2025

Host Information

IP: 192.168.50.3
MAC Address: 08:00:27:47:F1:70
OS: Linux Kernel 3.11.0-15-generic on Ubuntu 12.04

Vulnerabilities

77823 - Bash Remote Code Execution (Shellshock)

Synopsis

A system shell on the remote host is vulnerable to command injection.

Description

The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configuration of the system, an attacker could remotely execute arbitrary code.

See Also

http://seclists.org/oss-sec/2014/q3/650
http://www.nessus.org/u?dacf7829
https://www.invisiblethreat.ca/post/shellshock/

Solution

Update Bash.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.6

EPSS Score

0.9421

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	70103
CVE	CVE-2014-6271
XREF	EDB-ID:34765
XREF	EDB-ID:34766
XREF	IAVA:2014-A-0142
XREF	CISA-KNOWN-EXPLOITED:2022/07/28
XREF	CEA-ID:CEA-2019-0240

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/09/24, Modified: 2022/12/05

Plugin Output

tcp/22/ssh

```
Nessus was able to set the TERM environment variable used in an SSH
connection to :

() { :;}; /usr/bin/id > /tmp/nessus.1761730952

and read the output from the file :

uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)


Note: Nessus has attempted to remove the file /tmp/nessus.1761730952
```

201429 - Canonical Ubuntu Linux SEoL (12.04.x)

Synopsis

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

Description

According to its version, Canonical Ubuntu Linux is 12.04.x. It is, therefore, no longer maintained by its vendor or provider.

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

See Also

http://www.nessus.org/u?6c0a4182

Solution

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

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/0

```
OS                                    : Canonical Ubuntu Linux 12.04.4 LTS, Precise Pangolin
Security End of Life                  : April 28, 2017
Time since Security End of Life (Est.) : >= 8 years
```

118233 - MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU)

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.62. It is, therefore, affected by multiple vulnerabilities as noted in the October 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-62.html

http://www.nessus.org/u?705136d8

Solution

Upgrade to MySQL version 5.5.62 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0923

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-9843
CVE	CVE-2018-3133
CVE	CVE-2018-3174
CVE	CVE-2018-3282

Plugin Information

Published: 2018/10/19, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path              : /usr/sbin/mysqld
Installed version : 5.5.54-0ubuntu0.12.04.1
Fixed version     : 5.5.62
```

72598 - Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox regression (USN-2102-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2102-1 fixed vulnerabilities in Firefox. The update introduced a regression which could make Firefox crash under some circumstances.

This update fixes the problem.

We apologize for the inconvenience.

Christian Holler, Terrence Cole, Jesse Ruderman, Gary Kwong, Eric Rescorla, Jonathan Kew, Dan Gohman, Ryan VanderMeulen, Carsten Book, Andrew Sutherland, Byron Campen, Nicholas Nethercote, Paul Adenot, David Baron, Julian Seward and Sotaro Ikeda discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

(CVE-2014-1477, CVE-2014-1478)

Cody Crews discovered a method to bypass System Only Wrappers. An attacker could potentially exploit this to steal confidential data or execute code with the privileges of the user invoking Firefox. (CVE-2014-1479)

Jordi Chancel discovered that the downloads dialog did not implement a security timeout before button presses are processed. An attacker could potentially exploit this to conduct clickjacking attacks. (CVE-2014-1480)

Fredrik Lonnqvist discovered a use-after-free in Firefox.

An attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Firefox.

(CVE-2014-1482)

Jordan Milne discovered a timing flaw when using document.elementFromPoint and document.caretPositionFromPoint on cross-origin iframes. An attacker could potentially exploit this to steal confidential imformation. (CVE-2014-1483)

Frederik Braun discovered that the CSP implementation in Firefox did not handle XSLT stylesheets in accordance with the specification, potentially resulting in unexpected script execution in some circumstances (CVE-2014-1485)

Arthur Gerkis discovered a use-after-free in Firefox. An attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Firefox.

(CVE-2014-1486)

Masato Kinugawa discovered a cross-origin information leak in web worker error messages. An attacker could potentially exploit this to steal confidential information.

(CVE-2014-1487)

Yazan Tommalieh discovered that web pages could activate buttons on the default Firefox startpage (about:home) in some circumstances. An attacker could potentially exploit this to cause data loss by triggering a session restore.

(CVE-2014-1489)

Soeren Balko discovered a crash in Firefox when terminating web workers running asm.js code in some circumstances. An attacker could potentially exploit this to execute arbitrary code with the priviliges of the user invoking Firefox.

(CVE-2014-1488)

Several issues were discovered with ticket handling in NSS.

An attacker could potentially exploit these to cause a denial of service or bypass cryptographic protection mechanisms. (CVE-2014-1490, CVE-2014-1491)

Boris Zbarsky discovered that security restrictions on window objects could be bypassed under certain circumstances. (CVE-2014-1481).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2102-2/

Solution

Update the affected firefox package.

Risk Factor

Critical

VPR Score

6.7

EPSS Score

0.0889

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65316
BID	65320
BID	65321
BID	65322
BID	65326
BID	65328
BID	65329
BID	65330
BID	65331
BID	65332
BID	65334
BID	65335
CVE	CVE-2014-1477
CVE	CVE-2014-1478
CVE	CVE-2014-1479
CVE	CVE-2014-1480
CVE	CVE-2014-1481
CVE	CVE-2014-1482
CVE	CVE-2014-1483
CVE	CVE-2014-1485
CVE	CVE-2014-1486
CVE	CVE-2014-1487
CVE	CVE-2014-1488
CVE	CVE-2014-1489
CVE	CVE-2014-1490
CVE	CVE-2014-1491
XREF	USN:2102-2

Plugin Information

Published: 2014/02/20, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : firefox_26.0+build2-0ubuntu0.12.04.2
  - Fixed package     : firefox_27.0.1+build1-0ubuntu0.12.04.1
```

72425 - Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox vulnerabilities (USN-2102-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Christian Holler, Terrence Cole, Jesse Ruderman, Gary Kwong, Eric Rescorla, Jonathan Kew, Dan Gohman, Ryan VanderMeulen, Carsten Book, Andrew Sutherland, Byron Campen, Nicholas Nethercote, Paul Adenot, David Baron, Julian Seward and Sotaro Ikeda discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

(CVE-2014-1477, CVE-2014-1478)

Cody Crews discovered a method to bypass System Only Wrappers. An attacker could potentially exploit this to steal confidential data or execute code with the privileges of the user invoking Firefox.

(CVE-2014-1479)

Jordi Chancel discovered that the downloads dialog did not implement a security timeout before button presses are processed. An attacker could potentially exploit this to conduct clickjacking attacks.

(CVE-2014-1480)

Fredrik Lonnqvist discovered a use-after-free in Firefox. An attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Firefox. (CVE-2014-1482)

Jordan Milne discovered a timing flaw when using document.elementFromPoint and document.caretPositionFromPoint on cross-origin iframes. An attacker could potentially exploit this to steal confidential imformation. (CVE-2014-1483)

Frederik Braun discovered that the CSP implementation in Firefox did not handle XSLT stylesheets in accordance with the specification, potentially resulting in unexpected script execution in some circumstances (CVE-2014-1485)

Arthur Gerkis discovered a use-after-free in Firefox. An attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Firefox. (CVE-2014-1486)

Masato Kinugawa discovered a cross-origin information leak in web worker error messages. An attacker could potentially exploit this to steal confidential information. (CVE-2014-1487)

Yazan Tommalieh discovered that web pages could activate buttons on the default Firefox startpage (about:home) in some circumstances. An attacker could potentially exploit this to cause data loss by triggering a session restore. (CVE-2014-1489)

Soeren Balko discovered a crash in Firefox when terminating web workers running asm.js code in some circumstances. An attacker could potentially exploit this to execute arbitrary code with the priviliges of the user invoking Firefox. (CVE-2014-1488)

Several issues were discovered with ticket handling in NSS. An attacker could potentially exploit these to cause a denial of service or bypass cryptographic protection mechanisms. (CVE-2014-1490, CVE-2014-1491)

Boris Zbarsky discovered that security restrictions on window objects could be bypassed under certain circumstances. (CVE-2014-1481).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2102-1/

Solution

Update the affected firefox package.

Risk Factor

Critical

VPR Score

6.7

EPSS Score

0.0889

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65316
BID	65317
BID	65320
BID	65321
BID	65322
BID	65324
BID	65326
BID	65328
BID	65329
BID	65330
BID	65331

BID	65332
BID	65334
BID	65335
CVE	CVE-2014-1477
CVE	CVE-2014-1478
CVE	CVE-2014-1479
CVE	CVE-2014-1480
CVE	CVE-2014-1481
CVE	CVE-2014-1482
CVE	CVE-2014-1483
CVE	CVE-2014-1485
CVE	CVE-2014-1486
CVE	CVE-2014-1487
CVE	CVE-2014-1488
CVE	CVE-2014-1489
CVE	CVE-2014-1490
CVE	CVE-2014-1491
XREF	USN:2102-1

Plugin Information

Published: 2014/02/11, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : firefox_26.0+build2-0ubuntu0.12.04.2
  - Fixed package     : firefox_27.0+build1-0ubuntu0.12.04.1
```

72386 - Ubuntu 12.04 LTS / 12.10 / 13.10 : pidgin vulnerabilities (USN-2100-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Thijs Alkemade and Robert Vehse discovered that Pidgin incorrectly handled the Yahoo! protocol. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service.

(CVE-2012-6152)

Jaime Breva Ribes discovered that Pidgin incorrectly handled the XMPP protocol. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service. (CVE-2013-6477)

It was discovered that Pidgin incorrecly handled long URLs. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service. (CVE-2013-6478)

Jacob Appelbaum discovered that Pidgin incorrectly handled certain HTTP responses. A malicious remote server or a man in the middle could use this issue to cause Pidgin to crash, resulting in a denial of service. (CVE-2013-6479)

Daniel Atallah discovered that Pidgin incorrectly handled the Yahoo! protocol. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service. (CVE-2013-6481)

Fabian Yamaguchi and Christian Wressnegger discovered that Pidgin incorrectly handled the MSN protocol. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service.

(CVE-2013-6482)

Fabian Yamaguchi and Christian Wressnegger discovered that Pidgin incorrectly handled XMPP iq replies. A remote attacker could use this issue to spoof messages. (CVE-2013-6483)

It was discovered that Pidgin incorrectly handled STUN server responses. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service. (CVE-2013-6484)

Matt Jones discovered that Pidgin incorrectly handled certain chunked HTTP responses. A malicious remote server or a man in the middle could use this issue to cause Pidgin to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2013-6485)

Yves Younan and Ryan Pentney discovered that Pidgin incorrectly handled certain Gadu-Gadu HTTP messages. A malicious remote server or a man in the middle could use this issue to cause Pidgin to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2013-6487)

Yves Younan and Pawel Janic discovered that Pidgin incorrectly handled MXit emoticons. A remote attacker could use this issue to cause Pidgin to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2013-6489)

Yves Younan discovered that Pidgin incorrectly handled SIMPLE headers.

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

(CVE-2013-6490)

Daniel Atallah discovered that Pidgin incorrectly handled IRC argument parsing. A malicious remote server or a man in the middle could use this issue to cause Pidgin to crash, resulting in a denial of service.

(CVE-2014-0020).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2100-1/

Solution

Update the affected libpurple0 and / or pidgin packages.

Risk Factor

Critical

VPR Score

5.9

EPSS Score

0.5122

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

BID	65188
BID	65192
BID	65195
BID	65243
BID	65492
CVE	CVE-2012-6152
CVE	CVE-2013-6477
CVE	CVE-2013-6478
CVE	CVE-2013-6479
CVE	CVE-2013-6481

CVE	CVE-2013-6482
CVE	CVE-2013-6483
CVE	CVE-2013-6484
CVE	CVE-2013-6485
CVE	CVE-2013-6487
CVE	CVE-2013-6489
CVE	CVE-2013-6490
CVE	CVE-2014-0020
XREF	USN:2100-1

Plugin Information

Published: 2014/02/07, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libpurple0_1:2.10.3-0ubuntu1.3
  - Fixed package     : libpurple0_1:2.10.3-0ubuntu1.4
```

72599 - Ubuntu 12.04 LTS / 12.10 / 13.10 : thunderbird vulnerabilities (USN-2119-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Christian Holler, Terrence Cole, Jesse Ruderman, Gary Kwong, Eric Rescorla, Jonathan Kew, Dan Gohman, Ryan VanderMeulen and Sotaro Ikeda discovered multiple memory safety issues in Thunderbird. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1477)

Cody Crews discovered a method to bypass System Only Wrappers. If a user had enabled scripting, an attacker could potentially exploit this to steal confidential data or execute code with the privileges of the user invoking Thunderbird. (CVE-2014-1479)

Fredrik Lonnqvist discovered a use-after-free in Thunderbird. If a user had enabled scripting, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Thunderbird.

(CVE-2014-1482)

Arthur Gerkis discovered a use-after-free in Thunderbird. If a user had enabled scripting, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the priviliges of the user invoking Thunderbird.

(CVE-2014-1486)

Masato Kinugawa discovered a cross-origin information leak in web worker error messages. If a user had enabled scripting, an attacker could potentially exploit this to steal confidential information.

(CVE-2014-1487)

Several issues were discovered with ticket handling in NSS. An attacker could potentially exploit these to cause a denial of service or bypass cryptographic protection mechanisms. (CVE-2014-1490, CVE-2014-1491)

Boris Zbarsky discovered that security restrictions on window objects could be bypassed under certain circumstances. (CVE-2014-1481)

Fabian Cuchietti and Ateeq ur Rehman Khan discovered that it was possible to bypass JavaScript execution restrictions when replying to or forwarding mail messages in certain circumstances. An attacker could potentially exploit this to steal confidential information or modify message content. (CVE-2013-6674).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2119-1/

Solution

Update the affected thunderbird package.

Risk Factor

Critical

VPR Score

6.7

EPSS Score

0.3726

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65158
BID	65317
BID	65320
BID	65326
BID	65328
BID	65330
BID	65332
BID	65334
BID	65335
CVE	CVE-2013-6674
CVE	CVE-2014-1477
CVE	CVE-2014-1479
CVE	CVE-2014-1481
CVE	CVE-2014-1482
CVE	CVE-2014-1486
CVE	CVE-2014-1487
CVE	CVE-2014-1490
CVE	CVE-2014-1491
XREF	USN:2119-1

Plugin Information

Published: 2014/02/20, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : thunderbird_1:24.2.0+build1-0ubuntu0.12.04.1
  - Fixed package     : thunderbird_1:24.3.0+build2-0ubuntu0.12.04.1
```

81698 - Ubuntu 12.04 LTS : icu regression (USN-2522-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2522-1 fixed vulnerabilities in ICU. On Ubuntu 12.04 LTS, the font patches caused a regression when using LibreOffice Calc. The patches have been temporarily backed out until the regression is investigated.

We apologize for the inconvenience.

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 12.04 LTS. (CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2419)

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. (CVE-2014-6585, CVE-2014-6591)

It was discovered that ICU incorrectly handled memory operations when processing regular expressions. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

(CVE-2014-7923, CVE-2014-7926, CVE-2014-9654)

It was discovered that ICU collator implementation incorrectly handled memory operations. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. (CVE-2014-7940).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2522-2/

Solution

Update the affected libicu48 package.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.1776

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	59131
BID	59166
BID	59179
BID	59190
BID	72173
BID	72175
BID	72288
BID	72980
CVE	CVE-2013-1569
CVE	CVE-2013-2383
CVE	CVE-2013-2384
CVE	CVE-2013-2419
CVE	CVE-2014-6585
CVE	CVE-2014-6591
CVE	CVE-2014-7923
CVE	CVE-2014-7926
CVE	CVE-2014-7940
CVE	CVE-2014-9654
XREF	USN:2522-2

Plugin Information

Published: 2015/03/09, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libicu48_4.8.1.1-3ubuntu0.1
  - Fixed package     : libicu48_4.8.1.1-3ubuntu0.4
```

81754 - Ubuntu 12.04 LTS : icu vulnerabilities (USN-2522-3)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2522-1 fixed vulnerabilities in ICU. On Ubuntu 12.04 LTS, the font patches caused a regression when using LibreOffice Calc. The patches have now been updated to fix the regression.

We apologize for the inconvenience.

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 12.04 LTS. (CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2419)

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. (CVE-2014-6585, CVE-2014-6591)

It was discovered that ICU incorrectly handled memory operations when processing regular expressions. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

(CVE-2014-7923, CVE-2014-7926, CVE-2014-9654)

It was discovered that ICU collator implementation incorrectly handled memory operations. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. (CVE-2014-7940).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2522-3/

Solution

Update the affected libicu48 package.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:X/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.1776

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	59131
BID	59166
BID	59179
BID	59190
BID	72173
BID	72175
CVE	CVE-2013-1569
CVE	CVE-2013-2383
CVE	CVE-2013-2384
CVE	CVE-2013-2419
CVE	CVE-2014-6585
CVE	CVE-2014-6591
CVE	CVE-2014-7923
CVE	CVE-2014-7926
CVE	CVE-2014-7940
CVE	CVE-2014-9654
XREF	USN:2522-3

Plugin Information

Published: 2015/03/11, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libicu48_4.8.1.1-3ubuntu0.1
  - Fixed package     : libicu48_4.8.1.1-3ubuntu0.5
```

74213 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2225-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Matthew Daley reported an information leak in the floppy disk driver of the Linux kernel. An unprivileged local user could exploit this flaw to obtain potentially sensitive information from kernel memory.

(CVE-2014-1738)

Matthew Daley reported a flaw in the handling of ioctl commands by the floppy disk driver in the Linux kernel. An unprivileged local user could exploit this flaw to gain administrative privileges if the floppy disk module is loaded. (CVE-2014-1737)

A flaw was discovered in the vhost-net subsystem of the Linux kernel.

Guest OS users could exploit this flaw to cause a denial of service (host OS crash). (CVE-2014-0055)

A flaw was discovered in the handling of network packets when mergeable buffers are disabled for virtual machines in the Linux kernel. Guest OS users may exploit this flaw to cause a denial of service (host OS crash) or possibly gain privilege on the host OS.

(CVE-2014-0077)

Nikolay Aleksandrov discovered a race condition in Linux kernel's IPv4 fragment handling code. Remote attackers could exploit this flaw to cause a denial of service (system crash) or possibly have other unspecified impact. (CVE-2014-0100)

A flaw was discovered in the Linux kernel's handling of the SCTP handshake. A remote attacker could exploit this flaw to cause a denial of service (system crash). (CVE-2014-0101)

A flaw was discovered in the handling of routing information in Linux kernel's IPv6 stack. A remote attacker could exploit this flaw to cause a denial of service (memory consumption) via a flood of ICMPv6 router advertisement packets. (CVE-2014-2309)

An error was discovered in the Linux kernel's DCCP protocol support. A remote attacked could exploit this flaw to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2014-2523)

Max Sydorenko discovered a race condition in the Atheros 9k wireless driver in the Linux kernel. This race could be exploited by remote attackers to cause a denial of service (system crash). (CVE-2014-2672)

Adhemerval Zanella Neto discovered a flaw the in the Transactional Memory (TM) implementation for powerpc based machine. An unprivileged local user could exploit this flaw to cause a denial of service (system crash). (CVE-2014-2673)

An error was discovered in the Reliable Datagram Sockets (RDS) protocol stack in the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) or possibly have unspecified other impact. (CVE-2014-2678)

Yaara Rozenblum discovered a race condition in the Linux kernel's Generic IEEE 802.11 Networking Stack (mac80211). Remote attackers could exploit this flaw to cause a denial of service (system crash).

(CVE-2014-2706)

A flaw was discovered in the Linux kernel's ping sockets. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or possibly gain privileges via a crafted application. (CVE-2014-2851).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2225-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Critical

VPR Score

6.7

EPSS Score

0.0542

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65943
BID	66095
BID	66279
BID	66441
BID	66477
BID	66492
BID	66543
BID	66591
BID	66678
BID	66779

BID	67300
BID	67302
CVE	CVE-2014-0055
CVE	CVE-2014-0077
CVE	CVE-2014-0100
CVE	CVE-2014-0101
CVE	CVE-2014-1737
CVE	CVE-2014-1738
CVE	CVE-2014-2309
CVE	CVE-2014-2523
CVE	CVE-2014-2672
CVE	CVE-2014-2673
CVE	CVE-2014-2678
CVE	CVE-2014-2706
CVE	CVE-2014-2851
XREF	USN:2225-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/05/28, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-22.38~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

102814 - Ubuntu 12.04 LTS : python-crypto vulnerability (USN-3199-3)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-3199-1 fixed a vulnerability in Python Crypto. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that the ALGnew function in block_templace.c in the Python Cryptography Toolkit contained a heap-based buffer overflow vulnerability. A remote attacker could use this flaw to execute arbitrary code by using a crafted initialization vector parameter.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3199-3/

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.2012

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2013-7459
XREF	USN:3199-3

Plugin Information

Published: 2017/08/29, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : python-crypto_2.4.1-1ubuntu0.1
  - Fixed package     : python-crypto_2.4.1-1ubuntu0.2
```

101833 - Ubuntu 12.04 LTS : tiff vulnerabilities (USN-3212-3)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-3212-1 and USN-3212-2 fixed a vulnerabilitiy in LibTIFF. This update provides a subset of corresponding update for Ubuntu 12.04 ESM.

It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3212-3/

Solution

Update the affected libtiff-tools and / or libtiff4 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0894

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-7554
CVE	CVE-2015-8668
CVE	CVE-2016-10092
CVE	CVE-2016-3623
CVE	CVE-2016-3624
CVE	CVE-2016-3632
CVE	CVE-2016-3990
CVE	CVE-2016-3991
CVE	CVE-2016-5321
CVE	CVE-2016-5322
CVE	CVE-2016-8331
CVE	CVE-2016-9453
CVE	CVE-2016-9533
CVE	CVE-2016-9534
CVE	CVE-2016-9536
CVE	CVE-2016-9537
XREF	USN:3212-3

Plugin Information

Published: 2017/07/20, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.9.5-2ubuntu1.5
  - Fixed package     : libtiff4_3.9.5-2ubuntu1.10
```

102258 - Ubuntu 12.04 LTS : tiff vulnerabilities (USN-3212-4)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-3212-1 fixed several issues in LibTIFF. This update provides a subset of corresponding update for Ubuntu 12.04 ESM.

Mei Wang discovered a multiple integer overflows in LibTIFF which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write. (CVE-2016-3945)

It was discovered that LibTIFF is vulnerable to a heap buffer overflow in the resulting in DoS or code execution via a crafted BitsPerSample value. (CVE-2017-5225)

It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3212-4/

Solution

Update the affected libtiff-tools and / or libtiff4 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0097

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-3945
CVE	CVE-2017-5225
XREF	USN:3212-4

Plugin Information

Published: 2017/08/08, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.9.5-2ubuntu1.5
  - Fixed package     : libtiff4_3.9.5-2ubuntu1.11
```

146799 - Linux Sudo Privilege Escalation (Out-of-bounds Write)

Synopsis

The remote Linux distribution host is missing a security-related update.

Description

Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation to root via 'sudoedit -s' and a command-line argument that ends with a single backslash character.

See Also

https://www.sudo.ws/alerts/unescape_overflow.html

Solution

n/a.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.7

EPSS Score

0.9235

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3156
XREF	CISA-KNOWN-EXPLOITED:2022/04/27

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2021/02/24, Modified: 2025/10/20

Plugin Output

tcp/0

```
Nessus was able to prove the existence of a privilege escalation vulnerability by running the
 following command

/usr/bin/sudoedit -s / 2>&1

Nessus received the following response from the server:

sudoedit: /: not a regular file
```

106097 - MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU)

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.59. It is, therefore, affected by multiple vulnerabilities as noted in the January 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-59.html

http://www.nessus.org/u?ae82f1b1

http://www.nessus.org/u?17a0bb67

Solution

Upgrade to MySQL version 5.5.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	102495
BID	102706
BID	102678
BID	102681
BID	102682
BID	102713
CVE	CVE-2018-2562
CVE	CVE-2018-2622
CVE	CVE-2018-2640
CVE	CVE-2018-2665
CVE	CVE-2018-2668

Plugin Information

Published: 2018/01/17, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path              : /usr/sbin/mysqld
Installed version : 5.5.54-0ubuntu0.12.04.1
Fixed version     : 5.5.59
```

109166 - MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU)

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.60. It is, therefore, affected by multiple vulnerabilities as noted in the April 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-60.html

http://www.nessus.org/u?76507bf8

http://www.nessus.org/u?64303a9a

Solution

Upgrade to MySQL version 5.5.60 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.5

EPSS Score

0.0225

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	103778
BID	103802
BID	103804
BID	103814
BID	103824
BID	103828
BID	103830
CVE	CVE-2018-2755
CVE	CVE-2018-2758
CVE	CVE-2018-2761
CVE	CVE-2018-2766
CVE	CVE-2018-2771
CVE	CVE-2018-2773
CVE	CVE-2018-2781
CVE	CVE-2018-2782
CVE	CVE-2018-2784
CVE	CVE-2018-2787
CVE	CVE-2018-2805
CVE	CVE-2018-2813
CVE	CVE-2018-2817
CVE	CVE-2018-2818
CVE	CVE-2018-2819

Plugin Information

Published: 2018/04/19, Modified: 2024/10/30

Plugin Output

tcp/0

```
Path              : /usr/sbin/mysqld
Installed version : 5.5.54-0ubuntu0.12.04.1
Fixed version     : 5.5.60
```

73181 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : ca-certificates update (USN-2154-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 20130906 package.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2154-1/

Solution

Update the affected ca-certificates package.

Risk Factor

High

References

XREF	USN:2154-1

Plugin Information

Published: 2014/03/25, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : ca-certificates_20111211
  - Fixed package     : ca-certificates_20130906ubuntu0.12.04.1
```

72798 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3 vulnerability (USN-2125-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Ryan Smith-Roberts discovered that Python incorrectly handled buffer sizes when using the socket.recvfrom_into() function. An attacker could possibly use this issue to cause Python to crash, resulting in denial of service, or possibly execute arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2125-1/

Solution

Update the affected packages.

Risk Factor

High

VPR Score

6.4

EPSS Score

0.3144

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65379
CVE	CVE-2014-1912

XREF USN:2125-1

Plugin Information

Published: 2014/03/04, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : python2.7_2.7.3-0ubuntu3.4
- Fixed package     : python2.7_2.7.3-0ubuntu3.5

- Installed package : python2.7-minimal_2.7.3-0ubuntu3.4
- Fixed package     : python2.7-minimal_2.7.3-0ubuntu3.5
```

81042 - Ubuntu 10.04 LTS / 12.04 LTS : eglibc vulnerability (USN-2485-1) (GHOST)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that a buffer overflow existed in the gethostbyname and gethostbyname2 functions in the GNU C Library. An attacker could use this issue to execute arbitrary code or cause an application crash, resulting in a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2485-1/

Solution

Update the affected libc6 package.

Risk Factor

High

VPR Score

8.9

EPSS Score

0.8545

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-0235
XREF	CERT:967332
XREF	USN:2485-1

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2015/01/28, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libc6_2.15-0ubuntu10.5
  - Fixed package     : libc6_2.15-0ubuntu10.10
```

73092 - Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox vulnerabilities (USN-2150-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Benoit Jacob, Olli Pettay, Jan Varga, Jan de Mooij, Jesse Ruderman, Dan Gohman, Christoph Diehl, Gregor Wagner, Gary Kwong, Luke Wagner, Rob Fletcher and Makoto Kato discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1493, CVE-2014-1494)

Atte Kettunen discovered an out-of-bounds read during WAV file decoding. An attacker could potentially exploit this to cause a denial of service via application crash. (CVE-2014-1497)

David Keeler discovered that crypto.generateCRFMRequest did not correctly validate all arguments. An attacker could potentially exploit this to cause a denial of service via application crash.

(CVE-2014-1498)

Ehsan Akhgari discovered that the WebRTC permission dialog can display the wrong originating site information under some circumstances. An attacker could potentially exploit this by tricking a user in order to gain access to their webcam or microphone. (CVE-2014-1499)

Tim Philipp Schafers and Sebastian Neef discovered that onbeforeunload events used with page navigations could make the browser unresponsive in some circumstances. An attacker could potentially exploit this to cause a denial of service. (CVE-2014-1500)

Jeff Gilbert discovered that WebGL content could manipulate content from another sites WebGL context. An attacker could potentially exploit this to conduct spoofing attacks. (CVE-2014-1502)

Nicolas Golubovic discovered that CSP could be bypassed for data:

documents during session restore. An attacker could potentially exploit this to conduct cross-site scripting attacks. (CVE-2014-1504)

Robert O'Callahan discovered a mechanism for timing attacks involving SVG filters and displacements input to feDisplacementMap. An attacker could potentially exploit this to steal confidential information across domains. (CVE-2014-1505)

Tyson Smith and Jesse Schwartzentruber discovered an out-of-bounds read during polygon rendering in MathML. An attacker could potentially exploit this to steal confidential information across domains.

(CVE-2014-1508)

John Thomson discovered a memory corruption bug in the Cairo graphics library. If a user had a malicious extension installed, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1509)

Mariusz Mlynski discovered that web content could open a chrome privileged page and bypass the popup blocker in some circumstances. An attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1510, CVE-2014-1511)

It was discovered that memory pressure during garbage collection resulted in memory corruption in some circumstances. An attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1512)

Juri Aedla discovered out-of-bounds reads and writes with TypedArrayObject in some circumstances. An attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1513)

George Hotz discovered an out-of-bounds write with TypedArrayObject.

An attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2014-1514).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2150-1/

Solution

Update the affected firefox package.

Risk Factor

High

VPR Score

9.5

EPSS Score

0.7756

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66422
BID	66425
CVE	CVE-2014-1493
CVE	CVE-2014-1494
CVE	CVE-2014-1497
CVE	CVE-2014-1498
CVE	CVE-2014-1499

CVE	CVE-2014-1500
CVE	CVE-2014-1502
CVE	CVE-2014-1504
CVE	CVE-2014-1505
CVE	CVE-2014-1508
CVE	CVE-2014-1509
CVE	CVE-2014-1510
CVE	CVE-2014-1511
CVE	CVE-2014-1512
CVE	CVE-2014-1513
CVE	CVE-2014-1514
XREF	USN:2150-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2014/03/19, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : firefox_26.0+build2-0ubuntu0.12.04.2
  - Fixed package     : firefox_28.0+build2-0ubuntu0.12.04.1
```

73402 - Ubuntu 12.04 LTS / 12.10 / 13.10 : openssl vulnerabilities (USN-2165-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Neel Mehta discovered that OpenSSL incorrectly handled memory in the TLS heartbeat extension. An attacker could use this issue to obtain up to 64k of memory contents from the client or server, possibly leading to the disclosure of private keys and other sensitive information.

(CVE-2014-0160)

Yuval Yarom and Naomi Benger discovered that OpenSSL incorrectly handled timing during swap operations in the Montgomery ladder implementation. An attacker could use this issue to perform side-channel attacks and possibly recover ECDSA nonces.

(CVE-2014-0076).

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

VPR Score

6.9

EPSS Score

0.9447

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66363
CVE	CVE-2014-0076
CVE	CVE-2014-0160
XREF	USN:2165-1

XREF CISA-KNOWN-EXPLOITED:2022/05/25

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/04/08, Modified: 2022/05/05

Plugin Output

tcp/0

```
  - Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
  - Fixed package     : libssl1.0.0_1.0.1-4ubuntu5.12
```

73148 - Ubuntu 12.04 LTS / 12.10 / 13.10 : thunderbird vulnerabilities (USN-2151-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Benoit Jacob, Olli Pettay, Jan Varga, Jan de Mooij, Jesse Ruderman, Dan Gohman and Christoph Diehl discovered multiple memory safety issues in Thunderbird. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1493)

Atte Kettunen discovered an out-of-bounds read during WAV file decoding. If a user had enabled audio, an attacker could potentially exploit this to cause a denial of service via application crash.

(CVE-2014-1497)

Robert O'Callahan discovered a mechanism for timing attacks involving SVG filters and displacements input to feDisplacementMap. If a user had enabled scripting, an attacker could potentially exploit this to steal confidential information across domains. (CVE-2014-1505)

Tyson Smith and Jesse Schwartzentruber discovered an out-of-bounds read during polygon rendering in MathML. If a user had enabled scripting, an attacker could potentially exploit this to steal confidential information across domains. (CVE-2014-1508)

John Thomson discovered a memory corruption bug in the Cairo graphics library. If a user had a malicious extension installed, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1509)

Mariusz Mlynski discovered that web content could open a chrome privileged page and bypass the popup blocker in some circumstances. If a user had enabled scripting, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1510, CVE-2014-1511)

It was discovered that memory pressure during garbage collection resulted in memory corruption in some circumstances. If a user had enabled scripting, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1512)

Juri Aedla discovered out-of-bounds reads and writes with TypedArrayObject in some circumstances. If a user had enabled scripting, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2014-1513)

George Hotz discovered an out-of-bounds write with TypedArrayObject.

If a user had enabled scripting, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Thunderbird.

(CVE-2014-1514).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2151-1/

Solution

Update the affected thunderbird package.

Risk Factor

High

VPR Score

9.5

EPSS Score

0.7756

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66425
CVE	CVE-2014-1493
CVE	CVE-2014-1497
CVE	CVE-2014-1505
CVE	CVE-2014-1508
CVE	CVE-2014-1509
CVE	CVE-2014-1510
CVE	CVE-2014-1511
CVE	CVE-2014-1512
CVE	CVE-2014-1513
CVE	CVE-2014-1514
XREF	USN:2151-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2014/03/22, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : thunderbird_1:24.2.0+build1-0ubuntu0.12.04.1
  - Fixed package     : thunderbird_1:24.4.0+build1-0ubuntu0.12.04.1
```

73180 - Ubuntu 12.04 LTS / 12.10 : initramfs-tools vulnerability (USN-2153-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Kees Cook discovered that initramfs-tools incorrectly mounted /run without the noexec option, contrary to expected behaviour.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2153-1/

Solution

Update the affected initramfs-tools package.

Risk Factor

High

References

XREF	USN:2153-1

Plugin Information

Published: 2014/03/25, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : initramfs-tools_0.99ubuntu13.4
  - Fixed package     : initramfs-tools_0.99ubuntu13.5
```

100265 - Ubuntu 12.04 LTS : FreeType vulnerabilities (USN-3282-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, resulting in a denial of service, or possibly execute arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected libfreetype6 package.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.0114

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-8105
CVE	CVE-2017-8287
XREF	USN:3282-2

Plugin Information

Published: 2017/05/18, Modified: 2023/01/17

Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.4.8-1ubuntu2.1
  - Fixed package     : libfreetype6_2.4.8-1ubuntu2.6
```

97936 - Ubuntu 12.04 LTS : eglibc regression (USN-3239-3)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3239-1 fixed vulnerabilities in the GNU C Library. Unfortunately, the fix for CVE-2016-3706 introduced a regression that in some circumstances prevented IPv6 addresses from resolving. This update reverts the change in Ubuntu 12.04 LTS. We apologize for the error.

It was discovered that the GNU C Library incorrectly handled the strxfrm() function. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8982)

It was discovered that an integer overflow existed in the

_IO_wstr_overflow() function of the GNU C Library. An attacker could use this to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8983)

It was discovered that the fnmatch() function in the GNU C Library did not properly handle certain malformed patterns.

An attacker could use this to cause a denial of service.

This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8984)

Alexander Cherepanov discovered a stack-based buffer overflow in the glob implementation of the GNU C Library. An attacker could use this to specially craft a directory layout and cause a denial of service. (CVE-2016-1234)

Michael Petlan discovered an unbounded stack allocation in the getaddrinfo() function of the GNU C Library. An attacker could use this to cause a denial of service. (CVE-2016-3706)

Aldy Hernandez discovered an unbounded stack allocation in the sunrpc implementation in the GNU C Library. An attacker could use this to cause a denial of service. (CVE-2016-4429)

Tim Ruehsen discovered that the getaddrinfo() implementation in the GNU C Library did not properly track memory allocations. An attacker could use this to cause a denial of service. This issue only affected Ubuntu 16.04 LTS.

(CVE-2016-5417)

Andreas Schwab discovered that the GNU C Library on ARM 32-bit platforms did not properly set up execution contexts.

An attacker could use this to cause a denial of service.

(CVE-2016-6323).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3239-3/

Solution

Update the affected libc6 package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0135

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8982
CVE	CVE-2015-8983
CVE	CVE-2015-8984
CVE	CVE-2016-1234
CVE	CVE-2016-3706
CVE	CVE-2016-4429
CVE	CVE-2016-5417
CVE	CVE-2016-6323
XREF	USN:3239-3

Plugin Information

Published: 2017/03/24, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : libc6_2.15-0ubuntu10.5
  - Fixed package     : libc6_2.15-0ubuntu10.18
```

101148 - Ubuntu 12.04 LTS : eglibc vulnerability (USN-3323-2) (Stack Clash)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3323-1 fixed a vulnerability in the GNU C Library. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that the GNU C library did not properly handle memory when processing environment variables for setuid programs. A local attacker could use this in combination with another vulnerability to gain administrative privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected libc6 package. Note that the updated package may not be immediately available from the package repository or its mirrors.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.0673

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-1000366
XREF	USN:3323-2

Plugin Information

Published: 2017/06/30, Modified: 2025/04/02

Plugin Output

tcp/0

```
- Installed package : libc6_2.15-0ubuntu10.5
- Fixed package     : libc6_2.15-0ubuntu10.20
```

87238 - Ubuntu 12.04 LTS : foomatic-filters vulnerability (USN-2831-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Michal Kowalczyk discovered that the foomatic-filters foomatic-rip filter incorrectly stripped shell escape characters. A remote attacker could possibly use this issue to execute arbitrary code as the lp user.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2831-2/

Solution

Update the affected foomatic-filters package.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.1301

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8327
XREF	USN:2831-2

Plugin Information

Published: 2015/12/08, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : foomatic-filters_4.0.16-0ubuntu0.2
  - Fixed package     : foomatic-filters_4.0.16-0ubuntu0.3
```

87463 - Ubuntu 12.04 LTS : foomatic-filters vulnerability (USN-2838-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Adam Chester discovered that the foomatic-filters foomatic-rip filter incorrectly stripped shell escape characters. A remote attacker could possibly use this issue to execute arbitrary code as the lp user.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2838-2/

Solution

Update the affected foomatic-filters package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.4

EPSS Score

0.0481

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8560
XREF	USN:2838-2

Plugin Information

Published: 2015/12/17, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : foomatic-filters_4.0.16-0ubuntu0.2
- Fixed package     : foomatic-filters_4.0.16-0ubuntu0.4
```

100919 - Ubuntu 12.04 LTS : libnl3 vulnerability (USN-3311-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3311-1 fixed a vulnerability in libnl. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that libnl incorrectly handled memory when performing certain operations. A local attacker could possibly use this issue to cause libnl to crash, resulting in a denial of service, or execute arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected libnl-3-200 package. Note that the updated package may not be immediately available from the package repository and its mirrors.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0021

CVSS v2.0 Base Score

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

References

CVE	CVE-2017-0553
XREF	USN:3311-2

Plugin Information

Published: 2017/06/20, Modified: 2023/01/17

Plugin Output

tcp/0

```
  - Installed package : libnl-3-200_3.2.3-2ubuntu2
  - Fixed package     : libnl-3-200_3.2.3-2ubuntu2.1
```

92750 - Ubuntu 12.04 LTS : libreoffice vulnerability (USN-3046-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Yves Younan and Richard Johnson discovered that LibreOffice incorrectly handled presentation files. If a user were tricked into opening a specially crafted presentation file, a remote attacker could cause LibreOffice to crash, and possibly execute arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3046-1/

Solution

Update the affected libreoffice-core package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0062

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-1513
XREF	USN:3046-1

Plugin Information

Published: 2016/08/05, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : libreoffice-core_1:3.5.7-0ubuntu5
  - Fixed package     : libreoffice-core_1:3.5.7-0ubuntu12
```

72576 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2113-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Saran Neti reported a flaw in the ipv6 UDP Fragmentation Offload (UFI) in the Linux kernel. A remote attacker could exploit this flaw to cause a denial of service (panic). (CVE-2013-4563)

Mathy Vanhoef discovered an error in the the way the ath9k driver was handling the BSSID masking. A remote attacker could exploit this error to discover the original MAC address after a spoofing atack.

(CVE-2013-4579)

Andrew Honig reported a flaw in the Linux Kernel's kvm_vm_ioctl_create_vcpu function of the Kernel Virtual Machine (KVM) subsystem. A local user could exploit this flaw to gain privileges on the host machine. (CVE-2013-4587)

Andrew Honig reported a flaw in the apic_get_tmcct function of the Kernel Virtual Machine (KVM) subsystem if the Linux kernel. A guest OS user could exploit this flaw to cause a denial of service or host OS system crash. (CVE-2013-6367)

Andrew Honig reported an error in the Linux Kernel's Kernel Virtual Machine (KVM) VAPIC synchronization operation. A local user could exploit this flaw to gain privileges or cause a denial of service (system crash). (CVE-2013-6368)

Lars Bull discovered a flaw in the recalculate_apic_map function of the Kernel Virtual Machine (KVM) subsystem in the Linux kernel. A guest OS user could exploit this flaw to cause a denial of service (host OS crash). (CVE-2013-6376)

Nico Golde and Fabian Yamaguchi reported buffer underflow errors in the implementation of the XFS filesystem in the Linux kernel. A local user with CAP_SYS_ADMIN could exploit these flaw to cause a denial of service (memory corruption) or possibly other unspecified issues.

(CVE-2013-6382)

A flaw was discovered in the ipv4 ping_recvmsg function of the Linux kernel. A local user could exploit this flaw to cause a denial of service (NULL pointer dereference and system crash). (CVE-2013-6432)

mpd reported an information leak in the recvfrom, recvmmsg, and recvmsg system calls in the Linux kernel. An unprivileged local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7263)

mpb reported an information leak in the Layer Two Tunneling Protocol (l2tp) of the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7264)

mpb reported an information leak in the Phone Network protocol (phonet) in the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7265)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with ISDN sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7266)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with apple talk sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7267)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with ipx protocol sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7268)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with the netrom address family in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7269)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with packet address family sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7270)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with x25 protocol sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7271)

mpb reported an information leak in the Low-Rate Wireless Personal Area Networks support (IEEE 802.15.4) in the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7281)

halfdog reported an error in the AMD K7 and K8 platform support in the Linux kernel. An unprivileged local user could exploit this flaw on AMD based systems to cause a denial of service (task kill) or possibly gain privileges via a crafted application. (CVE-2014-1438)

An information leak was discovered in the Linux kernel's hamradio YAM driver for AX.25 packet radio. A local user with the CAP_NET_ADMIN capability could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-1446).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2113-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.149

CVSS v2.0 Base Score

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

References

CVE	CVE-2013-4563
CVE	CVE-2013-4579
CVE	CVE-2013-4587
CVE	CVE-2013-6367
CVE	CVE-2013-6368
CVE	CVE-2013-6376
CVE	CVE-2013-6382
CVE	CVE-2013-6432
CVE	CVE-2013-7263
CVE	CVE-2013-7264
CVE	CVE-2013-7265
CVE	CVE-2013-7266
CVE	CVE-2013-7267
CVE	CVE-2013-7268
CVE	CVE-2013-7269
CVE	CVE-2013-7270
CVE	CVE-2013-7271
CVE	CVE-2013-7281
CVE	CVE-2014-1438
CVE	CVE-2014-1446
XREF	USN:2113-1

Plugin Information

Published: 2014/02/19, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-17.31~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

73726 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2177-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

A flaw was discovered in the Kernel Virtual Machine (KVM) subsystem of the Linux kernel. A guest OS user could exploit this flaw to execute arbitrary code on the host OS. (CVE-2014-0049)

Al Viro discovered an error in how CIFS in the Linux kernel handles uncached write operations. An unprivileged local user could exploit this flaw to cause a denial of service (system crash), obtain sensitive information from kernel memory, or possibly gain privileges.

(CVE-2014-0069).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2177-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.0037

CVSS v2.0 Base Score

7.4 (CVSS2#AV:A/AC:M/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

BID	65588
BID	65909
CVE	CVE-2014-0049
CVE	CVE-2014-0069
XREF	USN:2177-1

Plugin Information

Published: 2014/04/27, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-20.34~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

74359 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2239-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Pinkie Pie discovered a flaw in the Linux kernel's futex subsystem. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or gain administrative privileges.

(CVE-2014-3153)

A flaw was discovered in the Linux kernel virtual machine's (kvm) validation of interrupt requests (irq). A guest OS user could exploit this flaw to cause a denial of service (host OS crash).

(CVE-2014-0155)

An information leak was discovered in the netfilter subsystem of the Linux kernel. An attacker could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-2568)

Sasha Levin reported a bug in the Linux kernel's virtual memory management subsystem. An unprivileged local user could exploit this flaw to cause a denial of service (system crash). (CVE-2014-3122).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2239-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

VPR Score

9.7

EPSS Score

0.8051

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2014-0155
CVE	CVE-2014-2568
CVE	CVE-2014-3122
CVE	CVE-2014-3153
XREF	USN:2239-1
XREF	CISA-KNOWN-EXPLOITED:2022/06/15

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/06/06, Modified: 2022/05/25

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-23.40~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

76566 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2287-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sasha Levin reported a flaw in the Linux kernel's point-to-point protocol (PPP) when used with the Layer Two Tunneling Protocol (L2TP).

A local user could exploit this flaw to gain administrative privileges. (CVE-2014-4943)

Michael S. Tsirkin discovered an information leak in the Linux kernel's segmentation of skbs when using the zerocopy feature of vhost-net. A local attacker could exploit this flaw to gain potentially sensitive information from kernel memory. (CVE-2014-0131)

An flaw was discovered in the Linux kernel's audit subsystem when auditing certain syscalls. A local attacker could exploit this flaw to obtain potentially sensitive single-bit values from kernel memory or cause a denial of service (OOPS). (CVE-2014-3917)

A flaw was discovered in the Linux kernel's implementation of user namespaces with respect to inode permissions. A local user could exploit this flaw by creating a user namespace to gain administrative privileges. (CVE-2014-4014)

Don Bailey discovered a flaw in the LZO decompress algorithm used by the Linux kernel. An attacker could exploit this flaw to cause a denial of service (memory corruption or OOPS). (CVE-2014-4608)

Don Bailey and Ludvig Strigeus discovered an integer overflow in the Linux kernel's implementation of the LZ4 decompression algorithm, when used by code not complying with API limitations. An attacker could exploit this flaw to cause a denial of service (memory corruption) or possibly other unspecified impact. (CVE-2014-4611).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2287-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

VPR Score

8.9

EPSS Score

0.1011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66101
BID	67699
BID	67988
BID	68214
BID	68218
BID	68683
CVE	CVE-2014-0131
CVE	CVE-2014-3917
CVE	CVE-2014-4014
CVE	CVE-2014-4608
CVE	CVE-2014-4611
CVE	CVE-2014-4943
XREF	USN:2287-1

Exploitable With

CANVAS (true)

Plugin Information

Published: 2014/07/17, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-26.45~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
```

```
fixes available.
```

78040 - Ubuntu 12.04 LTS : openssl update (USN-2367-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

For compatibility reasons, OpenSSL in Ubuntu 12.04 LTS disables TLSv1.2 by default when being used as a client. When forcing the use of TLSv1.2, another compatibility feature (OPENSSL_MAX_TLS1_2_CIPHER_LENGTH) was used that would truncate the cipher list. This would prevent certain ciphers from being selected, and would prevent secure renegotiations. This update removes the cipher list truncation workaround when forcing the use of TLSv1.2.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2367-1/

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

References

XREF	USN:2367-1

Plugin Information

Published: 2014/10/03, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
- Fixed package     : libssl1.0.0_1.0.1-4ubuntu5.18
```

83413 - Ubuntu 12.04 LTS : openssl update (USN-2606-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

For compatibility reasons, Ubuntu 12.04 LTS shipped OpenSSL with TLSv1.2 disabled when being used as a client.

This update re-enables TLSv1.2 by default now that the majority of problematic sites have been updated to fix compatibility issues.

For problematic environments, TLSv1.2 can be disabled again by setting the OPENSSL_NO_CLIENT_TLS1_2 environment variable before library initialization.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2606-1/

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

References

XREF	USN:2606-1

Plugin Information

Published: 2015/05/13, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
  - Fixed package     : libssl1.0.0_1.0.1-4ubuntu5.27
```

97722 - Ubuntu 12.04 LTS : python-imaging vulnerabilities (USN-3229-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that the Python Imaging Library incorrectly handled certain compressed text chunks in PNG images. A remote attacker could possibly use this issue to cause the Python Imaging Library to crash, resulting in a denial of service. (CVE-2014-9601)

Cris Neckar discovered that the Python Imaging Library incorrectly handled certain malformed images. A remote attacker could use this issue to cause the Python Imaging Library to crash, resulting in a denial of service, or possibly obtain sensitive information.

(CVE-2016-9189)

Cris Neckar discovered that the Python Imaging Library incorrectly handled certain malformed images. A remote attacker could use this issue to cause the Python Imaging Library to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9190).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3229-1/

Solution

Update the affected python-imaging package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0103

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2014-9601
CVE	CVE-2016-9189
CVE	CVE-2016-9190
XREF	USN:3229-1

Plugin Information

Published: 2017/03/14, Modified: 2023/01/12

Plugin Output

tcp/0

```
- Installed package : python-imaging_1.1.7-4
- Fixed package     : python-imaging_1.1.7-4ubuntu0.12.04.3
```

100379 - Ubuntu 12.04 LTS : rtmpdump vulnerabilities (USN-3283-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Dave McDaniel discovered that rtmpdump incorrectly handled certain malformed streams. If a user were tricked into processing a specially crafted stream, a remote attacker could cause rtmpdump to crash, resulting in a denial of service, or possibly execute arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected librtmp0 package. Note that the updated packages may not be immediately available from the package repository and its mirrors.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0111

CVSS v2.0 Base Score

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

References

CVE	CVE-2015-8270
CVE	CVE-2015-8271
CVE	CVE-2015-8272
XREF	USN:3283-2

Plugin Information

Published: 2017/05/24, Modified: 2023/01/17

Plugin Output

tcp/0

```
  - Installed package : librtmp0_2.4~20110711.gitc28f1bab-1
  - Fixed package     : librtmp0_2.4~20110711.gitc28f1bab-1ubuntu0.1
```

83346 - .bash_history Files Disclosed via Web Server

Synopsis

The remote web server hosts what may be a publicly accessible .bash_history file.

Description

Nessus has detected that the remote web server hosts publicly available files whose contents may be indicative of a typical bash history. Such files may contain sensitive information that should not be disclosed to the public.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information, and that the files are only accessible to those with valid credentials.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2015/05/12, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following .bash_history files are available on the remote server :

  - /.bash_history
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0032

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2025/02/11

Plugin Output

tcp/80/www

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "85c-b1-56686f37454ea"
  Inode number          : 2140
  File size             : 177 bytes
  File modification time : Mar.  3, 2018 at 19:17:59 GMT
```

111153 - MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU)

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.61. It is, therefore, affected by multiple vulnerabilities as noted in the July 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-61.html

http://www.nessus.org/u?50f36723

Solution

Upgrade to MySQL version 5.5.61 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0078

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	103954
BID	104766
BID	104779
BID	104786
CVE	CVE-2018-2767
CVE	CVE-2018-3058
CVE	CVE-2018-3063
CVE	CVE-2018-3066
CVE	CVE-2018-3070
CVE	CVE-2018-3081

Plugin Information

Published: 2018/07/20, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path              : /usr/sbin/mysqld
Installed version : 5.5.54-0ubuntu0.12.04.1
Fixed version     : 5.5.61
```

138561 - MySQL Denial of Service (Jul 2020 CPU)

Synopsis

The remote database server is affected by a denial of service vulnerability.

Description

The version of MySQL running on the remote host is 5.7.29 and prior or 8.0.19 and prior. It is, therefore, affected by a vulnerability, as noted in the July 2020 Critical Patch Update advisory:

A Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

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

See Also

http://www.nessus.org/u?dc7b9bd1

Solution

Refer to the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0037

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-14567
XREF	IAVA:2020-A-0321-S

Plugin Information

Published: 2020/07/16, Modified: 2023/11/01

Plugin Output

tcp/0

```
Path              : /usr/sbin/mysqld
Installed version : 5.5.54-0ubuntu0.12.04.1
Fixed version     : 5.7.30
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

73709 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : cups vulnerability (USN-2172-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Alex Korobkin discovered that the CUPS web interface incorrectly protected against cross-site scripting (XSS) attacks. If an authenticated user were tricked into visiting a malicious website while logged into CUPS, a remote attacker could modify the CUPS configuration and possibly steal confidential data.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2172-1/

Solution

Update the affected cups package.

Risk Factor

Medium

VPR Score

3.0

EPSS Score

0.0103

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66788
CVE	CVE-2014-2856
XREF	USN:2172-1

Plugin Information

Published: 2014/04/25, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : cups_1.5.3-0ubuntu8
  - Fixed package     : cups_1.5.3-0ubuntu8.2
```

73514 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Steve Holme discovered that libcurl incorrectly reused wrong connections when using protocols other than HTTP and FTP. This could lead to the use of unintended credentials, possibly exposing sensitive information. (CVE-2014-0138)

Richard Moore discovered that libcurl incorrectly validated wildcard SSL certificates that contain literal IP addresses. An attacker could possibly exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

(CVE-2014-0139).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2167-1/

Solution

Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0154

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66457
BID	66458
CVE	CVE-2014-0138
CVE	CVE-2014-0139
XREF	USN:2167-1

Plugin Information

Published: 2014/04/15, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libcurl3_7.22.0-3ubuntu4.7
- Fixed package     : libcurl3_7.22.0-3ubuntu4.8

- Installed package : libcurl3-gnutls_7.22.0-3ubuntu4.7
- Fixed package     : libcurl3-gnutls_7.22.0-3ubuntu4.8

- Installed package : libcurl3-nss_7.22.0-3ubuntu4.7
- Fixed package     : libcurl3-nss_7.22.0-3ubuntu4.8
```

72720 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerabilities (USN-2123-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that file incorrectly handled Composite Document files. An attacker could use this issue to cause file to crash, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS and Ubuntu 12.04 LTS. (CVE-2012-1571)

Bernd Melchers discovered that file incorrectly handled indirect offset values. An attacker could use this issue to cause file to consume resources or crash, resulting in a denial of service.

(CVE-2014-1943).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2123-1/

Solution

Update the affected file and / or libmagic1 packages.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.257

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	52225
BID	65596
CVE	CVE-2012-1571
CVE	CVE-2014-1943
XREF	USN:2123-1

Plugin Information

Published: 2014/02/27, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : file_5.09-2
- Fixed package     : file_5.09-2ubuntu0.2

- Installed package : libmagic1_5.09-2
- Fixed package     : libmagic1_5.09-2ubuntu0.2
```

73399 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that file incorrectly handled PE executable files.

An attacker could use this issue to cause file to crash, resulting in a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2162-1/

Solution

Update the affected file and / or libmagic1 packages.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.4346

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66002
CVE	CVE-2014-2270
XREF	USN:2162-1

Plugin Information

Published: 2014/04/08, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : file_5.09-2
  - Fixed package     : file_5.09-2ubuntu0.3

  - Installed package : libmagic1_5.09-2
  - Fixed package     : libmagic1_5.09-2ubuntu0.3
```

72812 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Nikos Mavrogiannopoulos discovered that GnuTLS incorrectly handled certificate verification functions. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited with specially crafted certificates to view sensitive information.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2127-1/

Solution

Update the affected libgnutls26 package.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0338

CVSS v2.0 Base Score

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

References

CVE	CVE-2014-0092
XREF	USN:2127-1

Plugin Information

Published: 2014/03/05, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libgnutls26_2.12.14-5ubuntu3.5
  - Fixed package     : libgnutls26_2.12.14-5ubuntu3.7
```

73513 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : net-snmp vulnerabilities (USN-2166-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Ken Farnen discovered that Net-SNMP incorrectly handled AgentX timeouts. A remote attacker could use this issue to cause the server to crash or to hang, resulting in a denial of service. (CVE-2012-6151)

It was discovered that the Net-SNMP ICMP-MIB incorrectly validated input. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service. This issue only affected Ubuntu 13.10. (CVE-2014-2284)

Viliam Pucik discovered that the Net-SNMP perl trap handler incorrectly handled NULL arguments. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service.

(CVE-2014-2285)

It was discovered that Net-SNMP incorrectly handled AgentX multi-object requests. A remote attacker could use this issue to cause the server to hang, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS, Ubuntu 12.04 LTS and Ubuntu 12.10.

(CVE-2014-2310).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2166-1/

Solution

Update the affected libsnmp15 and / or libsnmp30 packages.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.2215

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	64048
BID	65867
BID	65968
BID	66005
CVE	CVE-2012-6151
CVE	CVE-2014-2284
CVE	CVE-2014-2285
CVE	CVE-2014-2310
XREF	USN:2166-1

Plugin Information

Published: 2014/04/15, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libsnmp15_5.4.3~dfsg-2.4ubuntu1.1
  - Fixed package     : libsnmp15_5.4.3~dfsg-2.4ubuntu1.2
```

73316 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : nss vulnerability (USN-2159-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that NSS incorrectly handled wildcard certificates when used with internationalized domain names. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to spoof SSL servers.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2159-1/

Solution

Update the affected libnss3 and / or libnss3-1d packages.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0085

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66356
CVE	CVE-2014-1492
XREF	USN:2159-1

Plugin Information

Published: 2014/04/03, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libnss3_3.15.4-0ubuntu0.12.04.1
  - Fixed package     : libnss3_3.15.4-0ubuntu0.12.04.2
```

73556 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python-imaging vulnerabilities (USN-2168-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Jakub Wilk discovered that the Python Imaging Library incorrectly handled temporary files. A local attacker could possibly use this issue to overwrite arbitrary files, or gain access to temporary file contents. (CVE-2014-1932, CVE-2014-1933).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2168-1/

Solution

Update the affected python-imaging package.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.3 (CVSS2#E:U/RL:OF/RC:ND)

References

BID	65511
BID	65513
CVE	CVE-2014-1932

CVE	CVE-2014-1933
XREF	USN:2168-1

Plugin Information

Published: 2014/04/16, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : python-imaging_1.1.7-4
- Fixed package     : python-imaging_1.1.7-4ubuntu0.12.04.1
```

73016 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sebastien Macke discovered that Sudo incorrectly handled blacklisted environment variables when the env_reset option was disabled. A local attacker could use this issue to possibly run unintended commands by using blacklisted environment variables. In a default Ubuntu installation, the env_reset option is enabled by default. This issue only affected Ubuntu 10.04 LTS and Ubuntu 12.04 LTS. (CVE-2014-0106)

It was discovered that the Sudo init script set a date in the past on existing timestamp files instead of using epoch to invalidate them completely. A local attacker could possibly modify the system time to attempt to reuse timestamp files. This issue only applied to Ubuntu 12.04 LTS, Ubuntu 12.10 and Ubuntu 13.10. (LP: #1223297).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2146-1/

Solution

Update the affected sudo and / or sudo-ldap packages.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65997
CVE	CVE-2014-0106
XREF	USN:2146-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/03/14, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : sudo_1.8.3p1-1ubuntu3.4
- Fixed package     : sudo_1.8.3p1-1ubuntu3.6
```

72978 - Ubuntu 12.04 LTS / 12.10 / 13.10 : cups-filters vulnerabilities (USN-2143-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Florian Weimer discovered that cups-filters incorrectly handled memory in the urftopdf filter. An attacker could possibly use this issue to execute arbitrary code with the privileges of the lp user. This issue only affected Ubuntu 13.10. (CVE-2013-6473)

Florian Weimer discovered that cups-filters incorrectly handled memory in the pdftoopvp filter. An attacker could possibly use this issue to execute arbitrary code with the privileges of the lp user.

(CVE-2013-6474, CVE-2013-6475)

Florian Weimer discovered that cups-filters did not restrict driver directories in in the pdftoopvp filter. An attacker could possibly use this issue to execute arbitrary code with the privileges of the lp user. (CVE-2013-6476).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2143-1/

Solution

Update the affected cups-filters package.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0684

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	66161
CVE	CVE-2013-6473
CVE	CVE-2013-6474
CVE	CVE-2013-6475
CVE	CVE-2013-6476
XREF	USN:2143-1

Plugin Information

Published: 2014/03/13, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : cups-filters_1.0.18-0ubuntu0.1
  - Fixed package     : cups-filters_1.0.18-0ubuntu0.2
```

72701 - Ubuntu 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2121-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Suman Jana discovered that GnuTLS incorrectly handled version 1 intermediate certificates. This resulted in them being considered to be a valid CA certificate by default, which was contrary to documented behaviour.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2121-1/

Solution

Update the affected libgnutls26 package.

Risk Factor

Medium

VPR Score

3.5

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65559
CVE	CVE-2014-1959
XREF	USN:2121-1

Plugin Information

Published: 2014/02/26, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libgnutls26_2.12.14-5ubuntu3.5
  - Fixed package     : libgnutls26_2.12.14-5ubuntu3.6
```

73077 - Ubuntu 12.04 LTS / 12.10 / 13.10 : librsvg vulnerability (USN-2149-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that librsvg would load XML external entities by default. If a user were tricked into viewing a specially crafted SVG file, an attacker could possibly obtain access to arbitrary files.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2149-1/

Solution

Update the affected librsvg2-2 package.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0777

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	62714
CVE	CVE-2013-1881
XREF	USN:2149-1

Plugin Information

Published: 2014/03/18, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : librsvg2-2_2.36.1-0ubuntu1
  - Fixed package     : librsvg2-2_2.36.1-0ubuntu1.1
```

72925 - Ubuntu 12.04 LTS / 12.10 / 13.10 : udisks, udisks2 vulnerability (USN-2142-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Florian Weimer discovered that UDisks incorrectly handled certain long path names. A local attacker could use this issue to cause udisks to crash, resulting in a denial of service, or possibly execute arbitrary code. The default compiler options for affected releases should reduce the vulnerability to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2142-1/

Solution

Update the affected udisks and / or udisks2 packages.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66081
CVE	CVE-2014-0004
XREF	USN:2142-1

Plugin Information

Published: 2014/03/11, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : udisks_1.0.4-5ubuntu2.1
  - Fixed package     : udisks_1.0.4-5ubuntu2.2
```

73078 - Ubuntu 12.04 LTS / 12.10 : gtk+3.0 update (USN-2149-2)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2149-1 fixed a vulnerability in librsvg. This update provides a compatibility fix for GTK+ to work with the librsvg security update.

It was discovered that librsvg would load XML external entities by default. If a user were tricked into viewing a specially crafted SVG file, an attacker could possibly obtain access to arbitrary files.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2149-2/

Solution

Update the affected libgtk-3-0 package.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0777

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	62714

CVE	CVE-2013-1881
XREF	USN:2149-2

Plugin Information

Published: 2014/03/18, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libgtk-3-0_3.4.2-0ubuntu0.6
  - Fixed package     : libgtk-3-0_3.4.2-0ubuntu0.7
```

76707 - Ubuntu 12.04 LTS : acpi-support vulnerability (USN-2297-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

CESG discovered that acpi-support incorrectly handled certain privileged operations when checking for power management daemons. A local attacker could use this flaw to execute arbitrary code and elevate privileges to root.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2297-1/

Solution

Update the affected acpi-support package.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0011

CVSS v2.0 Base Score

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

References

CVE	CVE-2014-1419
XREF	USN:2297-1

Plugin Information

Published: 2014/07/23, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : acpi-support_0.140.1
  - Fixed package     : acpi-support_0.140.2
```

79120 - Ubuntu 12.04 LTS : libreoffice vulnerability (USN-2400-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that LibreOffice incorrectly handled OLE preview generation. If a user were tricked into opening a crafted document, an attacker could possibly exploit this to embed arbitrary data into documents.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2400-1/

Solution

Update the affected libreoffice-core package.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.114

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	69354
CVE	CVE-2014-3575
XREF	USN:2400-1

Plugin Information

Published: 2014/11/11, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libreoffice-core_1:3.5.7-0ubuntu5
  - Fixed package     : libreoffice-core_1:3.5.7-0ubuntu7
```

72900 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2137-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

An information leak was discovered in the Linux kernel when built with the NetFilter Connection Tracking (NF_CONNTRACK) support for IRC protocol (NF_NAT_IRC). A remote attacker could exploit this flaw to obtain potentially sensitive kernel information when communicating over a client- to-client IRC connection(/dcc) via a NAT-ed network.

(CVE-2014-1690)

Matthew Thode reported a denial of service vulnerability in the Linux kernel when SELinux support is enabled. A local user with the CAP_MAC_ADMIN capability (and the SELinux mac_admin permission if running in enforcing mode) could exploit this flaw to cause a denial of service (kernel crash). (CVE-2014-1874)

An information leak was discovered in the Linux kernel's NFS filesystem. A local users with write access to an NFS share could exploit this flaw to obtain potential sensative information from kernel memory. (CVE-2014-2038).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2137-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

VPR Score

4.2

EPSS Score

0.008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65180
BID	65688
CVE	CVE-2014-1690
CVE	CVE-2014-1874
CVE	CVE-2014-2038
XREF	USN:2137-1

Plugin Information

Published: 2014/03/10, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-18.32~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

76296 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2261-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Salva Peiro discovered an information leak in the Linux kernel's media- device driver. A local attacker could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-1739)

A bounds check error was discovered in the socket filter subsystem of the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) via crafted BPF instructions.

(CVE-2014-3144)

A remainder calculation error was discovered in the socket filter subsystem of the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) via crafted BPF instructions.

(CVE-2014-3145).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2261-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	67309
BID	67321
BID	68048
CVE	CVE-2014-1739
CVE	CVE-2014-3144
CVE	CVE-2014-3145
XREF	USN:2261-1

Plugin Information

Published: 2014/06/28, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-24.41~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

73890 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2201-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

A flaw was discovered in the Linux kernel's pseudo tty (pty) device.

An unprivileged user could exploit this flaw to cause a denial of service (system crash) or potentially gain administrator privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2201-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

VPR Score

8.8

EPSS Score

0.6902

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	67199
CVE	CVE-2014-0196

XREF USN:2201-1
XREF CISA-KNOWN-EXPLOITED:2023/06/02

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2014/05/06, Modified: 2023/05/14

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-20.35~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

76383 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2271-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Andy Lutomirski discovered a flaw with the Linux kernel's ptrace syscall on x86_64 processors. An attacker could exploit this flaw to cause a denial of service (System Crash) or potential gain administrative privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2271-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

VPR Score

7.4

EPSS Score

0.0152

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	68411
CVE	CVE-2014-4699
XREF	USN:2271-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/07/06, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
  - Fixed package     : linux-image-3.11.0-<ANY>-generic_3.11.0-24.42~precise1


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

87815 - Ubuntu 12.04 LTS : openssl vulnerability (USN-2863-1) (SLOTH)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Karthikeyan Bhargavan and Gaetan Leurent discovered that OpenSSL incorrectly allowed MD5 to be used for TLS 1.2 connections. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2863-1/

Solution

Update the affected libssl1.0.0 package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.02

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-7575
XREF	USN:2863-1

Plugin Information

Published: 2016/01/08, Modified: 2023/01/17

Plugin Output

tcp/0

```
  - Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
  - Fixed package     : libssl1.0.0_1.0.1-4ubuntu5.33
```

90021 - Ubuntu 12.04 LTS : pam regression (USN-2935-3)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2935-1 fixed vulnerabilities in PAM. The updates contained a packaging change that prevented upgrades in certain multiarch environments. USN-2935-2 intended to fix the problem but was incomplete for Ubuntu 12.04 LTS. This update fixes the problem in Ubuntu 12.04 LTS.

We apologize for the inconvenience.

It was discovered that the PAM pam_userdb module incorrectly used a case-insensitive method when comparing hashed passwords. A local attacker could possibly use this issue to make brute-force attacks easier. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2013-7041)

Sebastian Krahmer discovered that the PAM pam_timestamp module incorrectly performed filtering. A local attacker could use this issue to create arbitrary files, or possibly bypass authentication. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2014-2583)

Sebastien Macke discovered that the PAM pam_unix module incorrectly handled large passwords. A local attacker could possibly use this issue in certain environments to enumerate usernames or cause a denial of service. (CVE-2015-3238).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2935-3/

Solution

Update the affected libpam-modules package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0245

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2013-7041
CVE	CVE-2014-2583
CVE	CVE-2015-3238
XREF	USN:2935-3

Plugin Information

Published: 2016/03/18, Modified: 2023/01/12

Plugin Output

tcp/0

```
  - Installed package : libpam-modules_1.1.3-7ubuntu2
  - Fixed package     : libpam-modules_1.1.3-7ubuntu2.3
```

93559 - Ubuntu 12.04 LTS : python-imaging vulnerabilities (USN-3080-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Eric Soroos discovered that the Python Imaging Library incorrectly handled certain malformed FLI or PhotoCD files. A remote attacker could use this issue to cause Python Imaging Library to crash, resulting in a denial of service. (CVE-2016-0775, CVE-2016-2533)

Andrew Drake discovered that the Python Imaging Libray incorrectly validated input. A remote attacker could use this to cause Python Imaging Library to crash, resulting in a denial of service.

(CVE-2014-3589).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/3080-1/

Solution

Update the affected python-imaging package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0221

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2014-3589
CVE	CVE-2016-0775
CVE	CVE-2016-2533
XREF	USN:3080-1

Plugin Information

Published: 2016/09/16, Modified: 2023/01/12

Plugin Output

tcp/0

```
- Installed package : python-imaging_1.1.7-4
- Fixed package     : python-imaging_1.1.7-4ubuntu0.12.04.2
```

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.
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

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

VPR Score

1.4

EPSS Score

0.0307

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

77526 - Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Daniel Genkin, Adi Shamir, and Eran Tromer discovered that GnuPG was susceptible to an adaptive chosen ciphertext attack via physical side channels. A local attacker could use this attack to possibly recover private keys.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2339-1/

Solution

Update the affected gnupg package.

Risk Factor

Low

VPR Score

3.6

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	69164
CVE	CVE-2014-5270
XREF	USN:2339-1

Plugin Information

Published: 2014/09/04, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : gnupg_1.4.11-3ubuntu2.5
  - Fixed package     : gnupg_1.4.11-3ubuntu2.7
```

72980 - Ubuntu 12.04 LTS / 12.10 / 13.10 : libssh vulnerability (USN-2145-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Aris Adamantiadis discovered that libssh allowed the OpenSSL PRNG state to be reused when implementing forking servers. This could allow an attacker to possibly obtain information about the state of the PRNG and perform cryptographic attacks.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2145-1/

Solution

Update the affected libssh-4 package.

Risk Factor

Low

VPR Score

3.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65963
CVE	CVE-2014-0017
XREF	USN:2145-1

Plugin Information

Published: 2014/03/13, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libssh-4_0.5.2-1ubuntu0.12.04.2
  - Fixed package     : libssh-4_0.5.2-1ubuntu0.12.04.3
```

84794 - Ubuntu 12.04 LTS : firefox vulnerabilities (USN-2656-2) (Logjam)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2656-1 fixed vulnerabilities in Firefox for Ubuntu 14.04 LTS and later releases.

This update provides the corresponding update for Ubuntu 12.04 LTS.

Karthikeyan Bhargavan discovered that NSS incorrectly handled state transitions for the TLS state machine. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to skip the ServerKeyExchange message and remove the forward-secrecy property. (CVE-2015-2721)

Looben Yan discovered 2 use-after-free issues when using XMLHttpRequest in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-2722, CVE-2015-2733)

Bob Clary, Christian Holler, Bobby Holley, Andrew McCreight, Terrence Cole, Steve Fink, Mats Palmgren, Wes Kocher, Andreas Pehrson, Tooru Fujisawa, Andrew Sutherland, and Gary Kwong discovered multiple memory safety issues in Firefox.

If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-2724, CVE-2015-2725, CVE-2015-2726)

Armin Razmdjou discovered that opening hyperlinks with specific mouse and key combinations could allow a Chrome privileged URL to be opened without context restrictions being preserved. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass security restrictions.

(CVE-2015-2727)

Paul Bandha discovered a type confusion bug in the Indexed DB Manager. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the priviliges of the user invoking Firefox. (CVE-2015-2728)

Holger Fuhrmannek discovered an out-of-bounds read in Web Audio. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to obtain sensitive information. (CVE-2015-2729)

Watson Ladd discovered that NSS incorrectly handled Elliptical Curve Cryptography (ECC) multiplication. A remote attacker could possibly use this issue to spoof ECDSA signatures. (CVE-2015-2730)

A use-after-free was discovered when a Content Policy modifies the DOM to remove a DOM object. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the priviliges of the user invoking Firefox. (CVE-2015-2731)

Ronald Crane discovered multiple security vulnerabilities.

If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740)

David Keeler discovered that key pinning checks can be skipped when an overridable certificate error occurs. This allows a user to manually override an error for a fake certificate, but cannot be exploited on its own.

(CVE-2015-2741)

Jonas Jenwald discovered that some internal workers were incorrectly executed with a high privilege. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this in combination with another security vulnerability, to execute arbitrary code in a privileged scope. (CVE-2015-2743)

Matthew Green discovered a DHE key processing issue in NSS where a MITM could force a server to downgrade TLS connections to 512-bit export-grade cryptography. An attacker could potentially exploit this to impersonate the server. (CVE-2015-4000).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/2656-2/

Solution

Update the affected firefox package.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.9403

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

BID	75541
CVE	CVE-2015-2721
CVE	CVE-2015-2722
CVE	CVE-2015-2724
CVE	CVE-2015-2725
CVE	CVE-2015-2726
CVE	CVE-2015-2727
CVE	CVE-2015-2728
CVE	CVE-2015-2729
CVE	CVE-2015-2730
CVE	CVE-2015-2731
CVE	CVE-2015-2733
CVE	CVE-2015-2734
CVE	CVE-2015-2735
CVE	CVE-2015-2736
CVE	CVE-2015-2737
CVE	CVE-2015-2738
CVE	CVE-2015-2739
CVE	CVE-2015-2740
CVE	CVE-2015-2741
CVE	CVE-2015-2743
CVE	CVE-2015-4000
XREF	USN:2656-2
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/07/16, Modified: 2022/12/05

Plugin Output

tcp/0

```
  - Installed package : firefox_26.0+build2-0ubuntu0.12.04.2
  - Fixed package     : firefox_39.0+build5-0ubuntu0.12.04.2
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

141394 - Apache HTTP Server Installed (Linux)

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/10/21

Plugin Output

tcp/0

```
Nessus detected 4 installs of Apache:

  Path    : /usr/lib/apache2/mpm-worker/apache2
  Version : 2.2.22
  Running : no

  Configs found :

  Loaded modules :

  Path    : /usr/lib/apache2/mpm-event/apache2
  Version : 2.2.22
  Running : no

  Configs found :

  Loaded modules :
```

```
    Path    : /usr/lib/apache2/mpm-prefork/apache2
    Version : 2.2.22
    Running : no

    Configs found :

    Loaded modules :

    Path    : /usr/lib/apache2/mpm-itk/apache2
    Version : 2.2.22
    Running : no

    Configs found :

    Loaded modules :
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL        : http://192.168.50.3/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Version      : VirtualBox
Vendor       : innotek GmbH
Release Date : 12/01/2006
UUID         : CC4DE406-B99C-104B-B660-7BACFA3C4C0F
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:12.04.4::~~lts~~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:exiv2:libexiv2:0.22
  cpe:/a:gnupg:libgcrypt:1.5.0 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.22.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.22.0 -> Haxx libcurl
  cpe:/a:mysql:mysql:5.5.54-0ubuntu0.12.04.1_ -> MySQL MySQL
  cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:5.9p1 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.0.1 -> OpenSSL Project OpenSSL
  cpe:/a:php:php:5.3.10 -> PHP PHP
```

```
    cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ
    cpe:/a:vim:vim:7.3 -> Vim
```

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: 2025/10/20

Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 7.22.0
Associated Package : curl 7.22.0-3ubuntu4.17
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: 2025/10/20

Plugin Output

tcp/0

```
Hostname : bsides2018
  bsides2018 (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

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

Description

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

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

 - 192.168.50.3 (on interface eth1)
 - 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::a00:27ff:fe47:f170 (on interface eth1)
 - ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

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

Description

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

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

  - 08:00:27:47:f1:70 (interface eth1)
```

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
eth1:
  MAC : 08:00:27:47:f1:70
  IPv4:
    - Address : 192.168.50.3
      Netmask : 255.255.255.0
      Broadcast : 192.168.50.255
  IPv6:
    - Address : fe80::a00:27ff:fe47:f170
      Prefixlen : 64
      Scope : link
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Interface Routes:
  eth1:
    ipv4_subnets:
     - 169.254.0.0/16
     - 192.168.50.0/24
    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: 2025/10/20

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
```

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 :

08:00:27:47:F1:70 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:47:F1:70
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 2.3.5)
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /icons


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /icons

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Wed, 29 Oct 2025 09:31:03 GMT
  Server: Apache/2.2.22 (Ubuntu)
  Last-Modified: Sat, 03 Mar 2018 19:17:59 GMT
  ETag: "85c-b1-56686f37454ea"
  Accept-Ranges: bytes
  Content-Length: 177
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=98
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
```

```
</body></html>
```

171410 - IP Assignment Method Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/10/20

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eth1
  + IPv4
    - Address       : 192.168.50.3
      Assign Method : static
  + IPv6
    - Address       : fe80::a00:27ff:fe47:f170
      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: 2025/10/20

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /lib/i386-linux-gnu/libgcrypt.so.11
  Version : 1.5.0

  Path    : /lib/i386-linux-gnu/libgcrypt.so.11.7.0
  Version : 1.5.0
```

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
/dev/sda1       8.8G  2.5G  5.9G  30% /
udev            492M  4.0K  492M   1% /dev
tmpfs           201M  756K  200M   1% /run
none            5.0M     0  5.0M   0% /run/lock
none            501M     0  501M   0% /run/shm


$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0    10G  0 disk
|-sda1   8:1    0     9G  0 part /
|-sda2   8:2    0     1K  0 part
`-sda5   8:5    0  1022M  0 part [SWAP]
sr0     11:0    1  1024M  0 rom


$ mount -l
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
```

```
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
```

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: PDT -0700
Via /etc/timezone: America/Vancouver
Via /etc/localtime: PST8PDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
-----------[ User Accounts ]-----------

User         : abatchy
Home folder  : /home/abatchy
Start script : /bin/bash
Groups       : lpadmin
               cdrom
               sambashare
               sudo
               abatchy
               plugdev
               dip
               adm

User         : john
Home folder  : /home/john
Start script : /bin/bash
Groups       : john

User         : mai
Home folder  : /home/mai
Start script : /bin/bash
Groups       : mai

User         : anne
Home folder  : /home/anne
Start script : /bin/bash
Groups       : sudo
               anne
```

```
User         : doomguy
Home folder  : /home/doomguy
Start script : /bin/bash
Groups       : doomguy

----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

User         : daemon
Home folder  : /usr/sbin
Start script : /bin/sh
Groups       : daemon

User         : bin
Home folder  : /bin
Start script : /bin/sh
Groups       : bin

User         : sys
Home folder  : /dev
Start script : /bin/sh
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

User         : games
Home folder  : /usr/games
Start script : /bin/sh
Groups       : games

User         : man
Home folder  : /var/cache/man
Start script : /bin/sh
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : /bin/sh
Groups       : lp

User         : mail
Home folder  : /var/mail
Start script : /bin/sh
Groups       : mail

User         : news
Home folder  : /var/spool/news
Start script : /bin/sh
Groups       : news

User         : uucp
Home folder  : /var/spool/uucp
Start script : /bin/sh
Groups       : uucp

User         : proxy
Home folder  : /bin
Start script : /bin/sh
Groups       : proxy

User         : www-data
Home folder  : /var/www
```

```
Start script : /bin/sh
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /bin/sh
Groups       : backup

User         : list
Home folder  : /var/list
Start scrip [...]
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.50.3/
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.50.3/
```

129468 - MySQL Server Installed (Linux)

Synopsis

MySQL Server is installed on the remote Linux host.

Description

MySQL Server is installed on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/30, Modified: 2025/04/18

Plugin Output

tcp/0

```
Path    : /usr/sbin/mysqld
Version : 5.5.54-0ubuntu0.12.04.1
```

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: 2025/10/01

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.4
Nessus build : 20037
Plugin feed version : 202510211937
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Bsides-Vancouver-2018
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.100
Port scanner(s) : netstat
Port range : 0-65535
Ping RTT : 94.936 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'anne' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : some_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : port
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/10/29 10:29 CET (UTC +01:00)
Scan duration : 1009 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5353/mdns

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/33798

```
Port 33798/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/34849

```
Port 34849/udp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10

Remote operating system : Linux Kernel
Confidence level : 30
Method : mDNS
Type :
Fingerprint : mDNS:LINUX

Remote operating system : Linux Kernel 3.11.0-15-generic
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40
 UTC 2014 i686 i686 i386 GNU/Linux
```

```
Remote operating system : Linux Kernel 3.x on Ubuntu
Confidence level : 85
Method : HTTP
Type : general-purpose
Fingerprint : unknown

Remote operating system : Linux
Confidence level : 59
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B10113:F0x12:W29200:O0204ffff:M1460:
   P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191304_7_p=22

Remote operating system : Linux Kernel 3.11.0-15-generic on Ubuntu 12.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.11.0-15-generic on Ubuntu 12.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.11.0-15-generic on Ubuntu 12.04
```

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 bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686
 i386 GNU/Linux

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

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 17.38444 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  : anne
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: 2025/10/21

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 5.9p1
Banner  : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

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

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

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

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/10/20

Plugin Output

tcp/0

```
Nessus detected 3 installs of OpenSSL:

  Path               : /usr/bin/openssl
  Version            : 1.0.1
  Associated Package : openssl 1.0.1-4ubuntu5.11
  Managed by OS      : True

  Path               : /lib/i386-linux-gnu/libssl.so.1.0.0
  Version            : 1.0.1
  Associated Package : libssl1.0.0
```

```
  Path               : /lib/i386-linux-gnu/libcrypto.so.1.0.0
  Version            : 1.0.0
  Associated Package : libssl1.0.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these
 installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libatalla.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgmp.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
```

216936 - PHP Scripting Language Installed (Unix)

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly. Thorough test is required to get results on hosts running MacOS.

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/10/20

Plugin Output

tcp/0

```
Path               : /usr/bin/php5
Version            : 5.3.10
Associated Package : php5-cli: /usr/bin/php5
INI file           : /etc/php5/cli/php.ini
INI source         : PHP binary grep
Managed by OS      : True
```

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/10/14

Plugin Output

tcp/0

```
. You need to take the following 32 actions :

[ MySQL Denial of Service (Jul 2020 CPU) (138561) ]

+ Action to take : Refer to the vendor advisory.

+Impact : Taking this action will resolve 27 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : cups vulnerability (USN-2172-1) (73709) ]

+ Action to take : Update the affected cups package.

[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1) (73514) ]

+ Action to take : Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1) (73399) ]
```

```
+ Action to take : Update the affected file and / or libmagic1 packages.

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


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1) (72812) ]

+ Action to take : Update the affected libgnutls26 package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : net-snmp vulnerabilities (USN-2166-1) (73513) ]

+ Action to take : Update the affected libsnmp15 and / or libsnmp30 packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : nss vulnerability (USN-2159-1) (73316) ]

+ Action to take : Update the affected libnss3 and / or libnss3-1d packages.


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3
 vulnerability (USN-2125-1) (72798) ]

+ Action to take : Update the affected packages.


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1) (73016) ]

+ Action to take : Update the affected sudo and / or sudo-ldap packages.


[ Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1) (77526) ]

+ Action to take : Update the affected gnupg package.
 [...]
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/21/ftp

```
Process ID   : 898
Executable   : /usr/sbin/vsftpd
Command line : /usr/sbin/vsftpd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Process ID   : 422
Executable   : /usr/sbin/sshd
Command line : /usr/sbin/sshd -D
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/68

```
  Process ID   : 800
  Executable   : /sbin/dhclient
  Command line : /sbin/dhclient -d -4 -sf /usr/lib/NetworkManager/nm-dhcp-client.action -pf /
var/run/sendsigs.omit.d/network-manager.dhclient-eth1.pid -lf /var/lib/dhcp/dhclient-ecb765cd-
b2ba-4f58-9ada-f67d50a5b7dd-eth1.lease -cf /var/run/nm-dhclient-eth1.conf eth1
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/80/www

```
Process ID   : 1020
Executable   : /usr/lib/apache2/mpm-prefork/apache2
Command line : /usr/sbin/apache2 -k start
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/5353/mdns

```
Process ID   : 475
Executable   : /usr/sbin/avahi-daemon
Command line : avahi-daemon: running [bsides2018.local]
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/33798

```
Process ID   : 475
Executable   : /usr/sbin/avahi-daemon
Command line : avahi-daemon: running [bsides2018.local]
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/34849

```
Process ID   : 475
Executable   : /usr/sbin/avahi-daemon
Command line : avahi-daemon: running [bsides2018.local]
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-rsa
```

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

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

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

  hmac-sha1
  hmac-sha1-96

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

  hmac-sha1
  hmac-sha1-96
```

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_5.9p1 Debian-5ubuntu1.10
SSH supported authentication : publickey,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22869 - Software Enumeration (SSH)

Synopsis

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

Description

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

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

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

Plugin Output

tcp/0

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

  Desired=Unknown/Install/Remove/Purge/Hold
  | Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
  |/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
  ||/ Name
    Version
 Description
  +++-
==============================================================================-
==============================================================================-
==========================================================================================
  ii  accountsservice
    0.6.15-2ubuntu9.7
 query and manipulate user account information
  ii  acl
    2.2.51-5ubuntu1
 Access control list utilities
  ii  acpi-support
    0.140.1
 scripts for handling many ACPI events
```

```
 ii  acpid
   1:2.0.10-1ubuntu3
Advanced Configuration and Power Interface event daemon
 ii  activity-log-manager-common
   0.9.4-0ubuntu3.2
blacklist configuration for [...]
```

35351 - System Information Enumeration (via DMI)

Synopsis

Information about the remote system's hardware can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/12, Modified: 2025/03/18

Plugin Output

tcp/0

```
Chassis Information
  Serial Number : Not Specified
  Version       : Not Specified
  Manufacturer  : Oracle Corporation
  Lock          : Not Present
  Type          : Other

System Information
  Serial Number : VirtualBox-06e44dcc-9cb9-4b10-b660-7bacfa3c4c0f
  Version       : 1.2
  Manufacturer  : innotek GmbH
  Product Name  : VirtualBox
  Family        : Virtual Machine
```

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

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2025/08/28

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       'anne'
Port:       22
Proto:      SSH
Method:     password
Escalation: sudo
```

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:        'anne'
Port:        22
Proto:       SSH
Method:      password
Escalation: sudo
```

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  3.11.0-15-generi Wed Oct 29 02:12 - 02:33  (00:20)
reboot   system boot  3.11.0-15-generi Tue Oct 28 00:26 - 02:33 (1+02:07)
reboot   system boot  3.11.0-15-generi Mon Oct 27 08:17 - 02:33 (1+18:16)
reboot   system boot  3.11.0-15-generi Wed Oct 15 01:02 - 02:33 (14+01:30)
reboot   system boot  3.11.0-15-generi Tue Oct 14 07:03 - 02:33 (14+19:30)

wtmp begins Tue Oct 14 07:03:26 2025
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.50.100 to 192.168.50.3 :
192.168.50.100
192.168.50.3

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: 2025/10/20

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/bin/xz
  Version            : 5.1.1
  Associated Package : xz-utils 5.1.1alpha
  Confidence         : High
```

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

    Path               : /usr/lib/i386-linux-gnu/liblzma.so.5.0.0
    Version            : 5.1.1
    Associated Package : liblzma5 5.1.1alpha
    Confidence         : High
    Managed by OS      : True
    Version Source     : Package
```

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:
```

83303 - Unix / Linux - Local Users Information : Passwords Never Expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
  - abatchy
  - john
  - mai
  - anne
  - doomguy
```

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  0.1   3668  2032 ?        Ss   02:12   0:00 /sbin/init
root          2  0.0  0.0      0     0 ?        S    02:12   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    02:12   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   02:12   0:00 [kworker/0:0H]
root          7  0.0  0.0      0     0 ?        S    02:12   0:00 [migration/0]
root          8  0.0  0.0      0     0 ?        S    02:12   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    02:12   0:00 [rcu_sched]
root         10  0.0  0.0      0     0 ?        S    02:12   0:00 [watchdog/0]
root         11  0.0  0.0      0     0 ?        S<   02:12   0:00 [khelper]
root         12  0.0  0.0      0     0 ?        S    02:12   0:00 [kdevtmpfs]
root         13  0.0  0.0      0     0 ?        S<   02:12   0:00 [netns]
root         14  0.0  0.0      0     0 ?        S<   02:12   0:00 [writeback]
root         15  0.0  0.0      0     0 ?        S<   02:12   0:00 [kintegrityd]
root         16  0.0  0.0      0     0 ?        S<   02:12   0:00 [bioset]
root         17  0.0  0.0      0     0 ?        S<   02:12   0:00 [kworker/u3:0]
root         18  0.0  0.0      0     0 ?        S<   02:12   0:00 [kblockd]
root         19  0.0  0.0      0     0 ?        S<   02:12   0:00 [ata_sff]
root         20  0.0  0.0      0     0 ?        S    02:12   0:00 [khubd]
root         21  0.0  0.0      0     0 ?        S<   02:12   0:00 [md]
root         22  0.0  0.0      0     0 ?        S<   02:12   0:00 [devfreq_wq]
root         23  0.0  0.0      0     0 ?        S    02:12   0:01 [kworker/0:1]
root         25  0.0  0.0      0     0 ?        S    02:12   0:00 [khungtaskd]
root         26  0.0  0.0      0     0 ?        S    02:12   0:00 [kswapd0]
root         27  0.0  0.0      0     0 ?        SN   02:12   0:00 [ksmd]
root         28  0.0  0.0      0     0 ?        SN   02:12   0:00 [khugepaged]
root         29  0.0  0.0      0     0 ?        S    02:12   0:00 [fsn [...]
```

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  : anne
Protocol : SSH
```

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/10/20

Plugin Output

tcp/0

```
Path    : /usr/bin/vim.tiny
Version : 7.3
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.50.3/

Attached is a copy of the sitemap file.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/cgi-bin, /icons

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Contents of robots.txt :

User-agent: *
Disallow: /backup_wordpress
```

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: 2025/10/20

Plugin Output

tcp/0

```
Nessus detected 3 installs of libcurl:

  Path               : /usr/lib/i386-linux-gnu/libcurl.so.4.2.0
  Version            : 7.22.0
  Associated Package : libcurl3 7.22.0-3ubuntu4.7
  Managed by OS      : True

  Path               : /usr/lib/i386-linux-gnu/libcurl-nss.so.4.2.0
  Version            : 7.22.0
  Associated Package : libcurl3-nss 7.22.0-3ubuntu4.7
  Managed by OS      : True
```

```
    Path               : /usr/lib/i386-linux-gnu/libcurl-gnutls.so.4.2.0
    Version            : 7.22.0
    Associated Package : libcurl3-gnutls 7.22.0-3ubuntu4.7
    Managed by OS      : True
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/10/20

Plugin Output

tcp/0

```
Path               : /usr/lib/libexiv2.so.11.0.0
Version            : 0.22
Associated Package : libexiv2-11 0.22-2
Managed by OS      : True
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : bsides2018.local.

  - Advertised services :
    o Service name      : bsides2018 [08:00:27:47:f1:70]._workstation._tcp.local.
      Port number       : 9
    o Service name      : bsides2018._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : I686
  - OS                  : LINUX
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 2.3.5)
Version : 2.3.5
```