# ejer_2_tech__unidad_1_sprint_4

Report generated by Nessus™ Mon, 24 Jun 2024 03:46:39 CEST

TABLE OF CONTENTS

## Vulnerabilities by Host

# Vulnerabilities by Host

# 10.0.2.9

| 24 | 84 | 59 | 8 | 162 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

## Scan Information

Start time: Mon Jun 24 02:49:13 2024
End time: Mon Jun 24 03:46:39 2024

## Host Information

Netbios Name: METASPLOITABLE3-UB1404
IP: 10.0.2.9
MAC Address: 08:00:27:0E:2B:CC 66:17:FC:53:AF:9B 02:42:5D:B4:50:86
OS: Linux Kernel 3.13.0-24-generic on Ubuntu 14.04

## Vulnerabilities

### 92626 - Drupal Coder Module Deserialization RCE

#### Synopsis

A PHP application running on the remote web server is affected by a remote code execution vulnerability.

#### Description

The version of Drupal running on the remote web server is affected by a remote code execution vulnerability in the Coder module, specifically in file coder_upgrade.run.php, due to improper validation of user-supplied input to the unserialize() function. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary PHP code.

#### See Also

https://www.drupal.org/node/2765575

https://www.drupal.org/project/coder

#### Solution

Upgrade the Coder module to version 7.x-1.3 / 7.x-2.6 or later.

Alternatively, remove the entire Coder module directory from any publicly accessible website.

## Risk Factor

Critical

## 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:ND)

## References

XREF EDB-ID:40149

## Plugin Information

Published: 2016/07/29, Modified: 2022/04/11

## Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue using the following request :

http://10.0.2.9/drupal/sites/all/modules/coder/coder_upgrade/scripts/coder_upgrade.run.php


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
file parameter is not setNo path to parameter file

------------------------------ snip ------------------------------
```

## 81510 - PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.38. It is, therefore, affected by multiple vulnerabilities :

- A heap-based buffer overflow flaw in the enchant_broker_request_dict function in ext/enchant/enchant.c could allow a remote attacker to cause a buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2014-9705)

- A heap-based buffer overflow flaw in the GNU C Library (glibc) due to improperly validating user-supplied input in the glibc functions __nss_hostname_digits_dots(), gethostbyname(), and gethostbyname2(). This allows a remote attacker to cause a buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-0235)

- A use-after-free flaw exists in the function php_date_timezone_initialize_from_hash() within the 'ext/date/php_date.c' script. An attacker can exploit this to access sensitive information or crash applications linked to PHP. (CVE-2015-0273)

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

### See Also

http://php.net/ChangeLog-5.php#5.4.38

https://bugs.php.net/bug.php?id=68925

https://bugs.php.net/bug.php?id=68942

http://www.nessus.org/u?c7a6ddbd

### Solution

Upgrade to PHP version 5.4.38 or later.

### 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

9.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 72325 |
| BID | 72701 |
| BID | 73031 |
| CVE | CVE-2014-9705 |
| CVE | CVE-2015-0235 |
| CVE | CVE-2015-0273 |
| XREF | CERT:967332 |

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2015/02/25, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 82025 - PHP 5.4.x < 5.4.39 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.39. It is, therefore, affected by multiple vulnerabilities :

- A use-after-free error exists related to function 'unserialize', which can allow a remote attacker to execute arbitrary code. Note that this issue is due to an incomplete fix for CVE-2014-8142. (CVE-2015-0231)

- An integer overflow error exists in function 'regcomp'

in the Henry Spencer regex library, due to improper validation of user-supplied input. An attacker can exploit this to cause a denial of service or to execute arbitrary code. (CVE-2015-2305)

- An integer overflow error exists in the '_zip_cdir_new'

function, due to improper validation of user-supplied input. An attacker, using a crafted ZIP archive, can exploit this to cause a denial of service or to execute arbitrary code. (CVE-2015-2331)

- A filter bypass vulnerability exists due to a flaw in the move_uploaded_file() function in which pathnames are truncated when a NULL byte is encountered. This allows a remote attacker, via a crafted second argument, to bypass intended extension restrictions and create files with unexpected names. (CVE-2015-2348)

- A user-after-free error exists in the process_nested_data() function. This allows a remote attacker, via a crafted unserialize call, to dereference already freed memory, resulting in the execution of arbitrary code. (CVE-2015-2787)

- A type confusion vulnerability in the SoapClient's __call() function in ext/soap/soap.c could allow a remote attacker to execute arbitrary code by providing crafted serialized data with an unexpected data type (CVE-2015-4147, CVE-2015-4148)

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

### See Also

http://php.net/ChangeLog-5.php#5.4.39

https://bugs.php.net/bug.php?id=69207

https://bugs.php.net/bug.php?id=68976

### Solution

Upgrade to PHP version 5.4.39 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

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

VPR Score

8.8

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 | 72539 |
| BID | 73182 |
| BID | 73357 |
| BID | 73381 |
| BID | 73383 |
| BID | 73385 |
| BID | 73431 |
| BID | 73434 |
| BID | 75103 |
| CVE | CVE-2015-0231 |
| CVE | CVE-2015-2305 |
| CVE | CVE-2015-2331 |
| CVE | CVE-2015-2348 |
| CVE | CVE-2015-2787 |
| CVE | CVE-2015-4147 |
| CVE | CVE-2015-4148 |

Plugin Information

Published: 2015/03/24, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 83033 - PHP 5.4.x < 5.4.40 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x running on the remote web server is prior to 5.4.40. It is, therefore, affected by multiple vulnerabilities :

- An out-of-bounds read error exists in the GetCode_() function within file gd_gif_in.c that allows an unauthenticated, remote attacker to cause a denial of service condition or the disclosure of memory contents.

(CVE-2014-9709)

- A NULL pointer dereference flaw exists in the build_tablename() function within file pgsql.c in the PostgreSQL extension due to a failure to validate token extraction for table names. An authenticated, remote attacker can exploit this, via a crafted name, to cause a denial of service condition. (CVE-2015-1352)

- A use-after-free error exists in the phar_rename_archive() function within file phar_object.c. An unauthenticated, remote attacker can exploit this, by attempting to rename a phar archive to an already existing file name, to cause a denial of service condition. (CVE-2015-2301)

- An out-of-bounds read error exists in the Phar component due to improper validation of user-supplied input when handling phar parsing during unserialize() function calls. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the disclosure of memory contents. (CVE-2015-2783)

- A memory corruption issue exists in the phar_parse_metadata() function in file ext/phar/phar.c due to improper validation of user-supplied input when parsing a specially crafted TAR archive. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-3307)

- Multiple stack-based buffer overflow conditions exist in the phar_set_inode() function in file phar_internal.h when handling archive files, such as tar, zip, or phar files. An unauthenticated, remote attacker can exploit these to cause a denial of service condition or the execution or arbitrary code. (CVE-2015-3329)

- A flaw exists in the Apache2handler SAPI component when handling pipelined HTTP requests that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

(CVE-2015-3330)

- A flaw exists in multiple functions due to a failure to check for NULL byte (%00) sequences in a path when processing or reading a file. An unauthenticated, remote attacker can exploit this, via specially crafted input to an application calling those functions, to bypass intended restrictions and disclose potentially sensitive information. (CVE-2015-3411, CVE-2015-3412)

- A type confusion error exists in multiple functions within file ext/soap/soap.c that is triggered when calling unserialize(). An unauthenticated, remote attacker can exploit this to disclose memory contents, cause a denial of service condition, or execute arbitrary code. (CVE-2015-4599, CVE-2015-4600)

- Multiple type confusion errors exist within files ext/soap/php_encoding.c, ext/soap/php_http.c, and ext/soap/soap.c that allow an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-4601)

- A type confusion error exists in the

__PHP_Incomplete_Class() function within file ext/standard/incomplete_class.c that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

(CVE-2015-4602)

- A type confusion error exists in the exception::getTraceAsString() function within file Zend/zend_exceptions.c that allows a remote attacker to execute arbitrary code. (CVE-2015-4603)

- A denial of service vulnerability exists due to a flaw in the bundled libmagic library, specifically in the mget() function within file softmagic.c. The function fails to maintain a certain pointer relationship. An unauthenticated, remote attacker can exploit this, via a crafted string, to crash the application.

(CVE-2015-4604)

- A denial of service vulnerability exists due to a flaw in the bundled libmagic library, specifically in the mcopy() function within file softmagic.c. The function fails to properly handle an offset that exceeds 'bytecnt'. An unauthenticated, remote attacker can exploit this, via a crafted string, to crash the application. (CVE-2015-4605)

- A use-after-free error exists in the sqlite3_close() function within file /ext/sqlite3/sqlite3.c when closing database connections. An unauthenticated, remote attacker can exploit this to execute arbitrary code.

- A type confusion error exists in the php_stream_url_wrap_http_ex() function within file ext/standard/http_fopen_wrapper.c that allows an unauthenticated, remote attacker to execute arbitrary code.

- A use-after-free error exists in the php_curl() function within file ext/curl/interface.c that allows an unauthenticated, remote attacker to execute arbitrary code.

- A NULL pointer dereference flaw exists within file /ext/ereg/regex/regcomp.c that allows an unauthenticated, remote attacker attacker to cause a denial of service condition.

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

## See Also

http://php.net/ChangeLog-5.php#5.4.40

## Solution

Upgrade to PHP version 5.4.40 or later.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

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 | 71932 |
| BID | 73037 |
| BID | 73306 |
| BID | 74204 |
| BID | 74239 |
| BID | 74240 |
| BID | 74413 |
| BID | 74703 |
| BID | 75233 |
| BID | 75241 |
| BID | 75246 |
| BID | 75249 |
| BID | 75250 |
| BID | 75251 |
| BID | 75252 |
| BID | 75255 |
| CVE | CVE-2014-9709 |
| CVE | CVE-2015-1352 |
| CVE | CVE-2015-2301 |
| CVE | CVE-2015-2783 |
| CVE | CVE-2015-3307 |
| CVE | CVE-2015-3329 |
| CVE | CVE-2015-3330 |
| CVE | CVE-2015-3411 |
| CVE | CVE-2015-3412 |
| CVE | CVE-2015-4599 |
| CVE | CVE-2015-4600 |

| | |
|---|---|
| CVE | CVE-2015-4601 |
| CVE | CVE-2015-4602 |
| CVE | CVE-2015-4603 |
| CVE | CVE-2015-4604 |
| CVE | CVE-2015-4605 |

## Plugin Information

Published: 2015/04/23, Modified: 2024/05/28

## Plugin Output

tcp/80/www

## 83517 - PHP 5.4.x < 5.4.41 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x running on the remote web server is prior to 5.4.41. It is, therefore, affected by multiple vulnerabilities :

- Multiple unspecified flaws in pcrelib.

(CVE-2015-2325, CVE-2015-2326)

- A flaw in the phar_parse_tarfile function in ext/phar/tar.c could allow a denial of service via a crafted entry in a tar archive.

(CVE-2015-4021)

- An integer overflow condition exists in the ftp_genlist() function in ftp.c due to improper validation of user-supplied input. A remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or possible remote code execution. (CVE-2015-4022)

- Multiple flaws exist related to using pathnames containing NULL bytes. A remote attacker can exploit these flaws, by combining the '\0' character with a safe file extension, to bypass access restrictions. This had been previously fixed but was reintroduced by a regression in versions 5.4+. (CVE-2006-7243, CVE-2015-4025)

- A flaw exists in the multipart_buffer_headers() function in rfc1867.c due to improper handling of multipart/form-data in HTTP requests. A remote attacker can exploit this flaw to cause a consumption of CPU resources, resulting in a denial of service condition.

(CVE-2015-4024)

- A security bypass vulnerability exists due to a flaw in the pcntl_exec implementation that truncates a pathname upon encountering the '\x00' character. A remote attacker can exploit this, via a crafted first argument, to bypass intended extension restrictions and execute arbitrary files. (CVE-2015-4026)

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

### See Also

http://php.net/ChangeLog-5.php#5.4.41

### Solution

Upgrade to PHP version 5.4.41 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 44951 |
| BID | 74700 |
| BID | 74902 |
| BID | 74903 |
| BID | 74904 |
| BID | 75056 |
| BID | 75174 |
| BID | 75175 |
| CVE | CVE-2006-7243 |
| CVE | CVE-2015-2325 |
| CVE | CVE-2015-2326 |
| CVE | CVE-2015-4021 |
| CVE | CVE-2015-4022 |
| CVE | CVE-2015-4024 |
| CVE | CVE-2015-4025 |
| CVE | CVE-2015-4026 |

Plugin Information

Published: 2015/05/18, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 84362 - PHP 5.4.x < 5.4.42 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x running on the remote web server is prior to 5.4.42. It is, therefore, affected by multiple vulnerabilities :

- Multiple heap buffer overflow conditions exist in the bundled Perl-Compatible Regular Expression (PCRE) library due to improper validation of user-supplied input to the compile_branch() and pcre_compile2() functions. A remote attacker can exploit these conditions to cause a heap-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-2325, CVE-2015-2326)

- A denial of service vulnerability exists in the bundled SQLite component due to improper handling of quotes in collation sequence names. A remote attacker can exploit this to cause uninitialized memory access, resulting in denial of service condition.

(CVE-2015-3414)

- A denial of service vulnerability exists in the bundled SQLite component due to an improper implementation of comparison operators in the sqlite3VdbeExec() function in vdbe.c. A remote attacker can exploit this to cause an invalid free operation, resulting in a denial of service condition. (CVE-2015-3415)

- A denial of service vulnerability exists in the bundled SQLite component due to improper handling of precision and width values during floating-point conversions in the sqlite3VXPrintf() function in printf.c. A remote attacker can exploit this to cause a stack-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-3416)

- A security bypass vulnerability exists due to a failure in multiple extensions to check for NULL bytes in a path when processing or reading a file. A remote attacker can exploit this, by combining the '\0' character with a safe file extension, to bypass access restrictions.

(CVE-2015-4598)

- An arbitrary command injection vulnerability exists due to a flaw in the php_escape_shell_arg() function in exec.c. A remote attacker can exploit this, via the escapeshellarg() PHP method, to inject arbitrary operating system commands. (CVE-2015-4642)

- A heap buffer overflow condition exists in the ftp_genlist() function in ftp.c. due to improper validation of user-supplied input. A remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-4643)

- A denial of service vulnerability exists due to a NULL pointer dereference flaw in the build_tablename() function in pgsql.c. An authenticated, remote attacker can exploit this to cause an application crash.

(CVE-2015-4644)

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://php.net/ChangeLog-5.php#5.4.42

## Solution

Upgrade to PHP version 5.4.42 or later.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## 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 | 74228 |
| BID | 75174 |
| BID | 75175 |
| BID | 75244 |
| BID | 75290 |
| BID | 75291 |
| BID | 75292 |
| CVE | CVE-2015-2325 |
| CVE | CVE-2015-2326 |
| CVE | CVE-2015-3414 |
| CVE | CVE-2015-3415 |
| CVE | CVE-2015-3416 |
| CVE | CVE-2015-4598 |
| CVE | CVE-2015-4642 |
| CVE | CVE-2015-4643 |
| CVE | CVE-2015-4644 |

## Plugin Information

Published: 2015/06/24, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 84671 - PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x running on the remote web server is prior to 5.4.43. It is, therefore, affected by multiple vulnerabilities :

- A security feature bypass vulnerability, known as 'BACKRONYM', exists due to a failure to properly enforce the requirement of an SSL/TLS connection when the --ssl client option is used. A man-in-the-middle attacker can exploit this flaw to coerce the client to downgrade to an unencrypted connection, allowing the attacker to disclose data from the database or manipulate database queries. (CVE-2015-3152)

- A flaw in the phar_convert_to_other function in ext/phar/phar_object.c could allow a remote attacker to cause a denial of service. (CVE-2015-5589)

- A Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c could allow a remote attacker to cause a denial of service. (CVE-2015-5590)

- A flaw exists in the PHP Connector/C component due to a failure to properly enforce the requirement of an SSL/TLS connection when the --ssl client option is used.

A man-in-the-middle attacker can exploit this to downgrade the connection to plain HTTP when HTTPS is expected. (CVE-2015-8838)

- An unspecified flaw exists in the phar_convert_to_other() function in phar_object.c during the conversion of invalid TAR files. An attacker can exploit this flaw to crash a PHP application, resulting in a denial of service condition.

- A flaw exists in the parse_ini_file() and parse_ini_string() functions due to improper handling of strings that contain a line feed followed by an escape character. An attacker can exploit this to crash a PHP application, resulting in a denial of service condition.

- A user-after-free error exists in the object_custom() function in var_unserializer.c due to improper validation of user-supplied input. A remote attacker can exploit this to dereference already freed memory, potentially resulting in the execution of arbitrary code.

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://php.net/ChangeLog-5.php#5.4.43

http://backronym.fail/

### Solution

Upgrade to PHP version 5.4.43 or later.

### Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

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 | 74398 |
| BID | 75970 |
| BID | 75974 |
| BID | 88763 |
| CVE | CVE-2015-3152 |
| CVE | CVE-2015-5589 |
| CVE | CVE-2015-5590 |
| CVE | CVE-2015-8838 |

Plugin Information

Published: 2015/07/10, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 58987 - PHP Unsupported Version Detection

### Synopsis

The remote host contains an unsupported version of a web application scripting language.

### Description

According to its version, the installation of PHP on the remote host is no longer supported.

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

### See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

### Solution

Upgrade to a version of PHP 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)

### References

| | |
|---|---|
| XREF | IAVA:0001-A-0581 |

### Plugin Information

Published: 2012/05/04, Modified: 2024/05/31

### Plugin Output

tcp/80/www

## 84215 - ProFTPD mod_copy Information Disclosure

### Synopsis

The remote host is running a ProFTPD module that is affected by an information disclosure vulnerability.

### Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

### See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

### Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

### 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 | 74238 |

| | |
|---|---|
| CVE | CVE-2015-3306 |
| XREF | EDB-ID:36742 |
| XREF | EDB-ID:36803 |

## Exploitable With

CANVAS (true) Metasploit (true)

## Plugin Information

Published: 2015/06/16, Modified: 2024/01/16

## Plugin Output

tcp/21/ftp

## 194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

- less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically requires use with attacker-controlled file names, such as the files extracted from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases. (CVE-2024-32487)

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

### See Also

https://ubuntu.com/security/notices/USN-6756-1

### Solution

Update the affected less package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

7.3

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/0

## 193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6736-1 advisory.

- inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9840)

- inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9841)

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

- zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). (CVE-2022-37434)

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

### See Also

https://ubuntu.com/security/notices/USN-6736-1

### Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-9840 |
| CVE | CVE-2016-9841 |
| CVE | CVE-2018-25032 |
| CVE | CVE-2022-37434 |
| XREF | USN:6736-1 |

Plugin Information

Published: 2024/04/16, Modified: 2024/04/16

Plugin Output

tcp/0

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

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6762-1 advisory.

- nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd. (CVE-2014-9984)

- end_pattern (called from internal_fnmatch) in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash), as demonstrated by use of the fnmatch library function with the **(!() pattern. NOTE: this is not the same as CVE-2015-8984;

also, some Linux distributions have fixed CVE-2015-8984 but have not fixed this additional fnmatch issue.

(CVE-2015-20109)

- stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.

(CVE-2018-11236)

- A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and escalate their privileges on the system. (CVE-2021-3999)

- The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable. (CVE-2024-2961)

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

### See Also

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

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/0

## 83760 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2614-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2614-1 advisory.

- include/net/netfilter/nf_conntrack_extend.h in the netfilter subsystem in the Linux kernel before 3.14.5 uses an insufficiently large data type for certain extension data, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via outbound network traffic that triggers extension loading, as demonstrated by configuring a PPTP tunnel in a NAT environment. (CVE-2014-9715)

- Xen 3.3.x through 4.5.x and the Linux kernel through 3.19.1 do not properly restrict access to PCI command registers, which might allow local guest OS users to cause a denial of service (non-maskable interrupt and host crash) by disabling the (1) memory or (2) I/O decoding for a PCI Express device and then accessing the device, which triggers an Unsupported Request (UR) response. (CVE-2015-2150)

- arch/x86/kernel/entry_64.S in the Linux kernel before 3.19.2 does not prevent the TS_COMPAT flag from reaching a user-mode task, which might allow local users to bypass the seccomp or audit protection mechanism via a crafted application that uses the (1) fork or (2) close system call, as demonstrated by an attack against seccomp before 3.16. (CVE-2015-2830)

- The __driver_rfc4106_decrypt function in arch/x86/crypto/aesni-intel_glue.c in the Linux kernel before 3.19.3 does not properly determine the memory locations used for encrypted data, which allows context-dependent attackers to cause a denial of service (buffer overflow and system crash) or possibly execute arbitrary code by triggering a crypto API call, as demonstrated by use of a libkcapi test program with an AF_ALG(aead) socket. (CVE-2015-3331)

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

### See Also

https://ubuntu.com/security/notices/USN-2614-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 73014 |
| BID | 73699 |
| BID | 73953 |
| BID | 74235 |
| CVE | CVE-2014-9715 |
| CVE | CVE-2015-2150 |
| CVE | CVE-2015-2830 |
| CVE | CVE-2015-3331 |
| XREF | USN:2614-1 |

Plugin Information

Published: 2015/05/21, Modified: 2024/01/09

Plugin Output

tcp/0

## 90400 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2946-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2946-1 advisory.

- drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux kernel before 4.5 does not properly identify error conditions, which allows remote attackers to execute arbitrary code or cause a denial of service (use- after-free) via crafted packets. (CVE-2015-8812)

- The evm_verify_hmac function in security/integrity/evm/evm_main.c in the Linux kernel before 4.5 does not properly copy data, which makes it easier for local users to forge MAC values via a timing side-channel attack. (CVE-2016-2085)

- The Linux kernel before 4.5 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by leveraging incorrect tracking of descriptor ownership and sending each descriptor over a UNIX socket before closing it. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-4312. (CVE-2016-2550)

- fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes. (CVE-2016-2847)

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

### See Also

https://ubuntu.com/security/notices/USN-2946-1

### Solution

Update the affected kernel package.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-8812 |
| CVE | CVE-2016-2085 |
| CVE | CVE-2016-2550 |
| CVE | CVE-2016-2847 |
| XREF | USN:2946-1 |

Plugin Information

Published: 2016/04/07, Modified: 2024/01/09

Plugin Output

tcp/0

## 91425 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2989-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2989-1 advisory.

- The OZWPAN driver in the Linux kernel through 4.0.5 relies on an untrusted length field during packet parsing, which allows remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read and system crash) via a crafted packet. (CVE-2015-4004)

- Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU. (CVE-2016-2069)

- The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data. (CVE-2016-2117)

- The gtco_probe function in drivers/input/tablet/gtco.c in the Linux kernel through 4.5.2 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. (CVE-2016-2187)

- The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the intended restrictions on the ADDR_NO_RANDOMIZE flag, and bypass the ASLR protection mechanism for a setuid or setgid program, by disabling stack-consumption resource limits. (CVE-2016-3672)

- Double free vulnerability in drivers/net/usb/cdc_ncm.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (system crash) or possibly have unspecified other impact by inserting a USB device with an invalid USB descriptor. (CVE-2016-3951)

- The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted length value in a USB/IP packet. (CVE-2016-3955)

- The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory by reading a message. (CVE-2016-4485)

- The rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message. (CVE-2016-4486)

- fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls. (CVE-2016-4581)

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

### See Also

https://ubuntu.com/security/notices/USN-2989-1

## Solution

Update the affected kernel package.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2015-4004 |
| CVE | CVE-2016-2069 |
| CVE | CVE-2016-2117 |
| CVE | CVE-2016-2187 |
| CVE | CVE-2016-3672 |
| CVE | CVE-2016-3951 |
| CVE | CVE-2016-3955 |
| CVE | CVE-2016-4485 |
| CVE | CVE-2016-4486 |
| CVE | CVE-2016-4581 |
| XREF | USN:2989-1 |

## Plugin Information

Published: 2016/06/01, Modified: 2024/01/09

Plugin Output

tcp/0

## 101928 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3360-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3360-1 advisory.

- The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28803952 and Qualcomm internal bug CR570754. (CVE-2014-9900)

- The ioresources_init function in kernel/resource.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices, uses weak permissions for /proc/iomem, which allows local users to obtain sensitive information by reading this file, aka Android internal bug 28814213 and Qualcomm internal bug CR786116. NOTE: the permissions may be intentional in most non-Android contexts.

(CVE-2015-8944)

- arch/arm64/kernel/perf_event.c in the Linux kernel before 4.1 on arm64 platforms allows local users to gain privileges or cause a denial of service (invalid pointer dereference) via vectors involving events that are mishandled during a span of multiple HW PMUs. (CVE-2015-8955)

- Double free vulnerability in the sg_common_write function in drivers/scsi/sg.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (memory corruption and system crash) by detaching a device during an SG_IO ioctl call. (CVE-2015-8962)

- Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an swevent data structure during a CPU unplug operation. (CVE-2015-8963)

- The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure. (CVE-2015-8964)

- arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system call.

(CVE-2015-8966)

- arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the strict page permissions protection mechanism and modify the system-call table, and consequently gain privileges, by leveraging write access. (CVE-2015-8967)

- The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576. (CVE-2016-10088)

- sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.

(CVE-2017-1000380)

- The vmw_gb_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.7 does not validate certain levels data, which allows local users to cause a denial of service (system hang) via a crafted ioctl call for a /dev/dri/renderD* device. (CVE-2017-7346)

- The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.

(CVE-2017-7895)

- The edge_bulk_in_callback function in drivers/usb/serial/io_ti.c in the Linux kernel before 4.10.4 allows local users to obtain sensitive information (in the dmesg ringbuffer and syslog) from uninitialized kernel memory by using a crafted USB device (posing as an io_ti USB serial device) to trigger an integer underflow. (CVE-2017-8924)

- The omninet_open function in drivers/usb/serial/omninet.c in the Linux kernel before 4.10.4 allows local users to cause a denial of service (tty exhaustion) by leveraging reference count mishandling.

(CVE-2017-8925)

- The vmw_gb_surface_define_ioctl function (accessible via DRM_IOCTL_VMW_GB_SURFACE_CREATE) in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.11.4 defines a backup_handle variable but does not give it an initial value. If one attempts to create a GB surface, with a previously allocated DMA buffer to be used as a backup buffer, the backup_handle variable does not get written to and is then later returned to user space, allowing local users to obtain sensitive information from uninitialized kernel memory via a crafted ioctl call. (CVE-2017-9605)

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

## See Also

https://ubuntu.com/security/notices/USN-3360-1

## Solution

Update the affected kernel package.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2014-9900 |
| CVE | CVE-2015-8944 |
| CVE | CVE-2015-8955 |
| CVE | CVE-2015-8962 |
| CVE | CVE-2015-8963 |
| CVE | CVE-2015-8964 |
| CVE | CVE-2015-8966 |
| CVE | CVE-2015-8967 |
| CVE | CVE-2016-10088 |
| CVE | CVE-2017-1000380 |
| CVE | CVE-2017-7346 |
| CVE | CVE-2017-7895 |
| CVE | CVE-2017-8924 |
| CVE | CVE-2017-8925 |
| CVE | CVE-2017-9605 |
| XREF | USN:3360-1 |

### Plugin Information

Published: 2017/07/24, Modified: 2024/01/09

### Plugin Output

tcp/0

## 107003 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3583-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3583-1 advisory.

- A elevation of privilege vulnerability in the Upstream Linux file system. Product: Android. Versions:

Android kernel. Android ID: A-36817013. (CVE-2017-0750)

- Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors. (CVE-2017-0861)

- The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic. (CVE-2017-1000407)

- A security flaw was discovered in the nl80211_set_rekey_data() function in net/wireless/nl80211.c in the Linux kernel through 4.13.3. This function does not check whether the required attributes are present in a Netlink request. This request can be issued by a user with the CAP_NET_ADMIN capability and may result in a NULL pointer dereference and system crash. (CVE-2017-12153)

- The bio_map_user_iov and bio_unmap_user functions in block/bio.c in the Linux kernel before 4.13.8 do unbalanced refcounting when a SCSI I/O vector has small consecutive buffers belonging to the same page.

The bio_add_pc_page function merges them into one, but the page reference is never dropped. This causes a memory leak and possible system lockup (exploitable against the host OS by a guest OS user, if a SCSI disk is passed through to a virtual machine) due to an out-of-memory condition. (CVE-2017-12190)

- The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation. (CVE-2017-12192)

- An integer overflow in the qla2x00_sysfs_write_optrom_ctl function in drivers/scsi/qla2xxx/qla_attr.c in the Linux kernel through 4.12.10 allows local users to cause a denial of service (memory corruption and system crash) by leveraging root access. (CVE-2017-14051)

- The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR. (CVE-2017-14140)

- The atyfb_ioctl function in drivers/video/fbdev/aty/atyfb_base.c in the Linux kernel through 4.12.10 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading locations associated with padding bytes. (CVE-2017-14156)

- The iscsi_if_rx function in drivers/scsi/scsi_transport_iscsi.c in the Linux kernel through 4.13.2 allows local users to cause a denial of service (panic) by leveraging incorrect length validation.

(CVE-2017-14489)

- The tower_probe function in drivers/usb/misc/legousbtower.c in the Linux kernel before 4.8.1 allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.

(CVE-2017-15102)

- The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls.

(CVE-2017-15115)

- security/keys/keyctl.c in the Linux kernel before 4.11.5 does not consider the case of a NULL payload in conjunction with a nonzero length value, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted add_key or keyctl system call, a different vulnerability than CVE-2017-12192. (CVE-2017-15274)

- The bnep_add_connection function in net/bluetooth/bnep/core.c in the Linux kernel before 3.19 does not ensure that an l2cap socket is available, which allows local users to gain privileges via a crafted application. (CVE-2017-15868)

- The usb_serial_console_disconnect function in drivers/usb/serial/console.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device, related to disconnection and failed setup.

(CVE-2017-16525)

- net/netfilter/xt_osf.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for add_callback and remove_callback operations, which allows local users to bypass intended access restrictions because the xt_osf_fingers data structure is shared across all net namespaces.

(CVE-2017-17450)

- The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization. (CVE-2017-17806)

- The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.

(CVE-2017-18017)

- The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain rounding operation, which allows local users to map page zero, and consequently bypass a protection mechanism that exists for the mmap system call, by making crafted shmget and shmat system calls in a privileged context. (CVE-2017-5669)

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. (CVE-2017-5754)

- The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket. (CVE-2017-7542)

- The mm subsystem in the Linux kernel through 3.2 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c. (CVE-2017-7889)

- The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state. (CVE-2017-8824)

- In the Linux kernel through 4.14.13, the rds_cmsg_atomic function in net/rds/rdma.c mishandles cases where page pinning fails or an invalid address is supplied, leading to an rds_atomic_free_op NULL pointer dereference. (CVE-2018-5333)

- In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unspecified other impact. (CVE-2018-5344)

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

## See Also

https://ubuntu.com/security/notices/USN-3583-1

## Solution

Update the affected kernel package.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

8.1

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2017-0750 |
| CVE | CVE-2017-0861 |
| CVE | CVE-2017-1000407 |
| CVE | CVE-2017-12153 |
| CVE | CVE-2017-12190 |
| CVE | CVE-2017-12192 |
| CVE | CVE-2017-14051 |
| CVE | CVE-2017-14140 |
| CVE | CVE-2017-14156 |
| CVE | CVE-2017-14489 |
| CVE | CVE-2017-15102 |
| CVE | CVE-2017-15115 |
| CVE | CVE-2017-15274 |
| CVE | CVE-2017-15868 |
| CVE | CVE-2017-16525 |
| CVE | CVE-2017-17450 |
| CVE | CVE-2017-17806 |
| CVE | CVE-2017-18017 |
| CVE | CVE-2017-5669 |
| CVE | CVE-2017-5754 |
| CVE | CVE-2017-7542 |
| CVE | CVE-2017-7889 |
| CVE | CVE-2017-8824 |
| CVE | CVE-2018-5333 |
| CVE | CVE-2018-5344 |
| XREF | USN:3583-1 |
| XREF | IAVA:2018-A-0019 |

## Exploitable With

Metasploit (true)

## Plugin Information

Published: 2018/02/26, Modified: 2024/01/09

## Plugin Output

tcp/0

## 108843 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3620-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3620-1 advisory.

- In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a buffer overread is observed in nl80211_set_station when user space application sends attribute NL80211_ATTR_LOCAL_MESH_POWER_MODE with data of size less than 4 bytes (CVE-2017-11089)

- In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree. (CVE-2017-12762)

- net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list data structure is shared across all net namespaces.

(CVE-2017-17448)

- The KVM implementation in the Linux kernel through 4.14.7 allows attackers to obtain potentially sensitive information from kernel memory, aka a write_mmio stack-based out-of-bounds read, related to arch/x86/kvm/x86.c and include/trace/events/kvm.h. (CVE-2017-17741)

- The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable. (CVE-2017-17805)

- The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key to the current task's default request-key keyring via the request_key() system call, allowing a local user to use a sequence of crafted system calls to add keys to a keyring with only Search permission (not Write permission) to that keyring, related to construct_get_dest_keyring() in security/keys/request_key.c.

(CVE-2017-17807)

- Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..

(CVE-2018-1000026)

- In the Linux kernel through 3.2, the rds_message_alloc_sgs() function does not validate a value that is used during DMA page allocation, leading to a heap-based out-of-bounds write (related to the rds_rdma_extra_size function in net/rds/rdma.c). (CVE-2018-5332)

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

## See Also

https://ubuntu.com/security/notices/USN-3620-1

## Solution

Update the affected kernel package.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2017-11089 |
| CVE | CVE-2017-12762 |
| CVE | CVE-2017-17448 |
| CVE | CVE-2017-17741 |
| CVE | CVE-2017-17805 |
| CVE | CVE-2017-17807 |
| CVE | CVE-2018-1000026 |
| CVE | CVE-2018-5332 |
| XREF | USN:3620-1 |

## Plugin Information

Published: 2018/04/05, Modified: 2024/01/09

Plugin Output

tcp/0

## 112113 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3754-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3754-1 advisory.

- The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out- of-bounds read and system crash) via a crafted ext4 image. (CVE-2016-10208)

- The acpi_ns_terminate() function in drivers/acpi/acpica/nsutils.c in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table. (CVE-2017-11472)

- Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 3.2 allows local users to gain privileges via a crafted ACPI table. (CVE-2017-11473)

- The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel before 4.13.4 allows local users to obtain sensitive information from uninitialized kernel heap-memory locations via an SG_GET_REQUEST_TABLE ioctl call for /dev/sg0. (CVE-2017-14991)

- net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346. (CVE-2017-15649)

- drivers/uwb/uwbd.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16526)

- sound/usb/mixer.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (snd_usb_mixer_interrupt use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16527)

- The snd_usb_create_streams function in sound/usb/card.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16529)

- drivers/usb/core/config.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to the USB_DT_INTERFACE_ASSOCIATION descriptor. (CVE-2017-16531)

- The get_endpoints function in drivers/usb/misc/usbtest.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16532)

- The usbhid_parse function in drivers/hid/usbhid/hid-core.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16533)

- The usb_get_bos_descriptor function in drivers/usb/core/config.c in the Linux kernel before 4.13.10 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16535)

- The cx231xx_usb_probe function in drivers/media/usb/cx231xx/cx231xx-cards.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16536)

- The imon_probe function in drivers/media/rc/imon.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16537)

- drivers/media/usb/dvb-usb-v2/lmedm04.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device, related to a missing warm-start check and incorrect attach timing (dm04_lme2510_frontend_attach versus dm04_lme2510_tuner). (CVE-2017-16538)

- The parse_hid_report_descriptor function in drivers/input/tablet/gtco.c in the Linux kernel before 4.13.11 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16643)

- The hdpvr_probe function in drivers/media/usb/hdpvr/hdpvr-core.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (improper error handling and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16644)

- The ims_pcu_get_cdc_union_desc function in drivers/input/misc/ims-pcu.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (ims_pcu_parse_cdc_data out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16645)

- The qmi_wwan_bind function in drivers/net/usb/qmi_wwan.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16650)

- The vhci_hcd driver in the Linux Kernel before version 4.14.8 and 4.4.114 allows allows local attackers to disclose kernel memory addresses. Successful exploitation requires that a USB device is attached over IP.

(CVE-2017-16911)

- The get_pipe() function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 allows attackers to cause a denial of service (out-of-bounds read) via a specially crafted USB over IP packet. (CVE-2017-16912)

- The stub_recv_cmd_submit() function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 when handling CMD_SUBMIT packets allows attackers to cause a denial of service (arbitrary memory allocation) via a specially crafted USB over IP packet. (CVE-2017-16913)

- The stub_send_ret_submit() function (drivers/usb/usbip/stub_tx.c) in the Linux Kernel before version 4.14.8, 4.9.71, 4.1.49, and 4.4.107 allows attackers to cause a denial of service (NULL pointer dereference) via a specially crafted USB over IP packet. (CVE-2017-16914)

- The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux kernel through 4.14.5 does not consider the maximum number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-17558)

- The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation. (CVE-2017-18255)

- In the Linux kernel before 4.13.5, a local user could create keyrings for other users via keyctl commands, setting unwanted defaults or causing a denial of service. (CVE-2017-18270)

- The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a MOV SS, NULL selector instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application. (CVE-2017-2583)

- arch/x86/kvm/emulate.c in the Linux kernel through 4.9.3 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free) via a crafted application that leverages instruction emulation for fxrstor, fxsave, sgdt, and sidt. (CVE-2017-2584)

- The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call. (CVE-2017-2671)

- The klsi_105_get_line_state function in drivers/usb/serial/kl5kusb105.c in the Linux kernel before 4.9.5 places uninitialized heap-memory contents into a log entry upon a failure to read the line status, which allows local users to obtain sensitive information by reading the log. (CVE-2017-5549)

- The ip6gre_err function in net/ipv6/ip6_gre.c in the Linux kernel allows remote attackers to have unspecified impact via vectors involving GRE flags in an IPv6 packet, which trigger an out-of-bounds access. (CVE-2017-5897)

- The LLC subsystem in the Linux kernel before 4.9.13 does not ensure that a certain destructor exists in required circumstances, which allows local users to cause a denial of service (BUG_ON) or possibly have unspecified other impact via crafted system calls. (CVE-2017-6345)

- The hashbin_delete function in net/irda/irqueue.c in the Linux kernel before 4.9.13 improperly manages lock dropping, which allows local users to cause a denial of service (deadlock) via crafted operations on IrDA devices. (CVE-2017-6348)

- A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFLAGS during emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A user/process inside a guest could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by this. (CVE-2017-7518)

- The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c. (CVE-2017-7645)

- The saa7164_bus_get function in drivers/media/pci/saa7164/saa7164-bus.c in the Linux kernel through 4.11.5 allows local users to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact by changing a certain sequence-number value, aka a double fetch vulnerability.

(CVE-2017-8831)

- The snd_msnd_interrupt function in sound/isa/msnd/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a double fetch vulnerability. (CVE-2017-9984)

- The snd_msndmidi_input_read function in sound/isa/msnd/msnd_midi.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a double fetch vulnerability. (CVE-2017-9985)

- Linux Kernel version 3.18 to 4.16 incorrectly handles an SG_IO ioctl on /dev/sg0 with dxfer_direction=SG_DXFER_FROM_DEV and an empty 6-byte cmdp. This may lead to copying up to 1000

kernel heap pages to the userspace. This has been fixed upstream in https://github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824 already. The problem has limited scope, as users don't usually have permissions to access SCSI devices. On the other hand, e.g. the Nero user manual suggests doing `chmod o+r+w /dev/sg*` to make the devices accessible. NOTE: third parties dispute the relevance of this report, noting that the requirement for an attacker to have both the CAP_SYS_ADMIN and CAP_SYS_RAWIO capabilities makes it virtually impossible to exploit. (CVE-2018-1000204)

- drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows local users to cause a denial of service (ata qc leak) by triggering certain failure conditions. NOTE: a third party disputes the relevance of this report because the failure can only occur for physically proximate attackers who unplug SAS Host Bus Adapter cables (CVE-2018-10021)

- The kernel_wait4 function in kernel/exit.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service by triggering an attempted use of the -INT_MIN value. (CVE-2018-10087)

- The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument. (CVE-2018-10124)

- The xfs_bmap_extents_to_btree function in fs/xfs/libxfs/xfs_bmap.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_bmapi_write NULL pointer dereference) via a crafted xfs image. (CVE-2018-10323)

- The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls. (CVE-2018-10675)

- Linux kernel ext4 filesystem is vulnerable to an out-of-bound access in the ext4_ext_drop_refs() function when operating on a crafted ext4 filesystem image. (CVE-2018-10877)

- A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image. (CVE-2018-10881)

- The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image. (CVE-2018-1092)

- The ext4_valid_block_bitmap function in fs/ext4/balloc.c in the Linux kernel through 4.15.15 allows attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image because balloc.c and ialloc.c do not validate bitmap block numbers. (CVE-2018-1093)

- The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory. (CVE-2018-10940)

- In the ea_get function in fs/jfs/xattr.c in the Linux kernel through 4.17.1, a memory corruption bug in JFS can be triggered by calling setxattr twice with two different extended attribute names on the same file. This vulnerability can be triggered by an unprivileged user with the ability to create files and execute programs. A kmalloc call is incorrect, leading to slab-out-of-bounds in jfs_xattr.

(CVE-2018-12233)

- An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp. (CVE-2018-13094)

- The inode_init_owner function in fs/inode.c in the Linux kernel through 3.16 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is

writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID. (CVE-2018-13405)

- An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used. (CVE-2018-13406)

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

### See Also

https://ubuntu.com/security/notices/USN-3754-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2016-10208 |
| CVE | CVE-2017-11472 |
| CVE | CVE-2017-11473 |
| CVE | CVE-2017-14991 |

| | |
|---|---|
| CVE | CVE-2017-15649 |
| CVE | CVE-2017-16526 |
| CVE | CVE-2017-16527 |
| CVE | CVE-2017-16529 |
| CVE | CVE-2017-16531 |
| CVE | CVE-2017-16532 |
| CVE | CVE-2017-16533 |
| CVE | CVE-2017-16535 |
| CVE | CVE-2017-16536 |
| CVE | CVE-2017-16537 |
| CVE | CVE-2017-16538 |
| CVE | CVE-2017-16643 |
| CVE | CVE-2017-16644 |
| CVE | CVE-2017-16645 |
| CVE | CVE-2017-16650 |
| CVE | CVE-2017-16911 |
| CVE | CVE-2017-16912 |
| CVE | CVE-2017-16913 |
| CVE | CVE-2017-16914 |
| CVE | CVE-2017-17558 |
| CVE | CVE-2017-18255 |
| CVE | CVE-2017-18270 |
| CVE | CVE-2017-2583 |
| CVE | CVE-2017-2584 |
| CVE | CVE-2017-2671 |
| CVE | CVE-2017-5549 |
| CVE | CVE-2017-5897 |
| CVE | CVE-2017-6345 |
| CVE | CVE-2017-6348 |
| CVE | CVE-2017-7518 |
| CVE | CVE-2017-7645 |
| CVE | CVE-2017-8831 |
| CVE | CVE-2017-9984 |
| CVE | CVE-2017-9985 |
| CVE | CVE-2018-1000204 |
| CVE | CVE-2018-10021 |
| CVE | CVE-2018-10087 |
| CVE | CVE-2018-10124 |
| CVE | CVE-2018-10323 |
| CVE | CVE-2018-10675 |
| CVE | CVE-2018-10877 |
| CVE | CVE-2018-10881 |
| CVE | CVE-2018-1092 |

| | |
|---|---|
| CVE | CVE-2018-1093 |
| CVE | CVE-2018-10940 |
| CVE | CVE-2018-12233 |
| CVE | CVE-2018-13094 |
| CVE | CVE-2018-13405 |
| CVE | CVE-2018-13406 |
| XREF | USN:3754-1 |

## Plugin Information

Published: 2018/08/24, Modified: 2024/01/09

## Plugin Output

tcp/0

## 85801 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2734-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2734-1 advisory.

- Integer overflow in the sg_start_req function in drivers/scsi/sg.c in the Linux kernel 2.6.x through 4.x before 4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large iov_count value in a write request. (CVE-2015-5707)

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

### See Also

https://ubuntu.com/security/notices/USN-2734-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-5707 |
| XREF | USN:2734-1 |

Plugin Information

Published: 2015/09/04, Modified: 2024/01/09

Plugin Output

tcp/0

## 96980 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3188-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3188-1 advisory.

- The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data. (CVE-2016-9555)

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

### See Also

https://ubuntu.com/security/notices/USN-3188-1

### Solution

Update the affected kernel package.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-9555 |
| XREF | USN:3188-1 |

Plugin Information

Published: 2017/02/03, Modified: 2024/01/09

Plugin Output

tcp/0

## 125851 - Ubuntu 14.04 LTS : glib2.0 vulnerability (USN-4014-2)

### Synopsis

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

### Description

USN-4014-1 fixed a vulnerability in GLib. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.

Original advisory details :

It was discovered that GLib incorrectly handled certain files. An attacker could possibly use this issue to access 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/4014-2/

### Solution

Update the affected libglib2.0-0, libglib2.0-bin and / or libglib2.0-dev packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2019-12450 |
| XREF | USN:4014-2 |

Plugin Information

Published: 2019/06/12, Modified: 2024/05/16

Plugin Output

tcp/0

## 33850 - Unix Operating System Unsupported Version Detection

### Synopsis

The operating system running on the remote host is no longer supported.

### Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

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

### Solution

Upgrade to a version of the Unix operating system 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)

### References

| | |
|---|---|
| XREF | IAVA:0001-A-0502 |
| XREF | IAVA:0001-A-0648 |

### Plugin Information

Published: 2008/08/08, Modified: 2024/06/14

### Plugin Output

tcp/0

```
Ubuntu 14.04 support ended on 2019-04-30 (end of maintenance) / 2024-04-30 (end of extended security
 maintenance).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

## 125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

### Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

### Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

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

### See Also

http://www.nessus.org/u?c9d7fc8c

### Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

### 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

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 108617 |
| CVE | CVE-2019-11768 |

Plugin Information

Published: 2019/06/13, Modified: 2024/06/04

Plugin Output

tcp/80/www

## 42424 - CGI Generic SQL Injection (blind)

### Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

### Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

### See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://www.nessus.org/u?11ab1866

### Solution

Modify the affected CGI scripts so that they properly escape arguments.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:77 |
| XREF | CWE:89 |
| XREF | CWE:91 |
| XREF | CWE:203 |
| XREF | CWE:643 |
| XREF | CWE:713 |
| XREF | CWE:722 |

| | |
|---|---|
| XREF | CWE:727 |
| XREF | CWE:751 |
| XREF | CWE:801 |
| XREF | CWE:810 |
| XREF | CWE:928 |
| XREF | CWE:929 |

## Plugin Information

Published: 2009/11/06, Modified: 2024/06/14

## Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'js_frame' parameter of the /phpmyadmin/phpmyadmin.css.php CGI :

/phpmyadmin/phpmyadmin.css.php?token=69830204c8eac460ae41291389c9868c&no
cache=4334846010&server=1&js_frame=rightzz69830204c8eac460ae41291389c986
8c&nocache=4334846010&server=1&js_frame=rightyy
+ The 'q' parameter of the /drupal/ CGI :

/drupal/?form_id=user_login_block&destination=node&form_build_id=form-d8
LdjYn0RUG0TOJvGyqs1cbfT5g2VZRXrV9DuvGs4YA&pass=&op=Log%20in&name=&q=rss.
xmlzzuser_login_block&destination=node&form_build_id=form-d8LdjYn0RUG0TO
JvGyqs1cbfT5g2VZRXrV9DuvGs4YA&pass=&op=Log%20in&name=&q=rss.xmlyy

Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'password' parameter of the /payroll_app.php CGI :

/payroll_app.php [user=&s=OK&password='+or+'1'='1]
```

## 78515 - Drupal Database Abstraction API SQLi

### Synopsis

The remote web server is running a PHP application that is affected by a SQL injection vulnerability.

### Description

The remote web server is running a version of Drupal that is affected by a SQL injection vulnerability due to a flaw in the Drupal database abstraction API, which allows a remote attacker to use specially crafted requests that can result in arbitrary SQL execution. This may lead to privilege escalation, arbitrary PHP execution, or remote code execution.

### See Also

https://www.drupal.org/SA-CORE-2014-005

https://www.drupal.org/project/drupal/releases/7.32

### Solution

Upgrade to version 7.32 or later.

### Risk Factor

High

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 70595 |
| CVE | CVE-2014-3704 |
| XREF | EDB-ID:34984 |
| XREF | EDB-ID:34992 |
| XREF | EDB-ID:34993 |
| XREF | EDB-ID:35150 |

## Exploitable With

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

## Plugin Information

Published: 2014/10/16, Modified: 2022/04/11

## Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue using the following request :

POST /drupal/?q=node&destination=node HTTP/1.1
Host: 10.0.2.9
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 117
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
name[0;SELECT
+@@version;#]=0;&name[0]=nessus&pass=nessus&test2=test&form_build_id=&form_id=user_login_block&op=Log
+in


This produced the following truncated output (limited to 5 lines) :
------------------------------ snip ------------------------------
>Warning</em>: mb_strlen() expects parameter 1 to be string, array given in <em
 class="placeholder">drupal_strlen()</em> (line <em class="placeholder">441</em> of <em
 class="placeholder">/var/www/html/drupal/includes/unicode.inc</em>).</li>
<li><em class="placeholder">Warning</em>: addcslashes() expects parameter 1 to be string,
 array given in <em class="placeholder">DatabaseConnection-&gt;escapeLike()</em> (line <em
 class="placeholder">965</em> of <em class="placeholder">/var/www/html/drupal/includes/database/
database.inc</em>).</li>
<li>Sorry, too many failed login attempts from your IP address. This IP address is temporarily
 blocked. Try again later or <a href="/drupal/?q=user/password">request a new password</a>.</li>
</ul>
</div>
[...]

------------------------------ snip ------------------------------
```

## 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

### 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: 2024/06/21

## Plugin Output

tcp/0

## 66585 - PHP 5.4.x < 5.4.13 Information Disclosure

### Synopsis

The remote web server uses a version of PHP that is potentially affected by an information disclosure vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.13. It is, therefore, potentially affected by an information disclosure vulnerability. The 5.4.12 fix for CVE-2013-1635 / CVE-2013-1643 was incomplete and an error still exists in the files 'ext/soap/php_xml.c' and 'ext/libxml/libxml.c' related to handling external entities. This error could cause PHP to parse remote XML documents defined by an attacker and could allow access to arbitraryfiles.

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

### See Also

http://www.nessus.org/u?7c770707

http://www.php.net/ChangeLog-5.php#5.4.13

### Solution

Upgrade to PHP version 5.4.13 or later.

### 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

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 58224 |
| BID | 58766 |
| BID | 62373 |
| CVE | CVE-2013-1635 |
| CVE | CVE-2013-1643 |
| CVE | CVE-2013-1824 |

Plugin Information

Published: 2013/05/24, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 67260 - PHP 5.4.x < 5.4.17 Buffer Overflow

### Synopsis

The remote web server uses a version of PHP that is potentially affected by a buffer overflow vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.17. It is, therefore, potentially affected by a buffer overflow error that exists in the function '_pdo_pgsql_error' in the file 'ext/pdo_pgsql/pgsql_driver.c'.

Note that this plugin does not attempt to exploit this vulnerability, but instead, relies only on PHP's self-reported version number.

### See Also

https://bugs.php.net/bug.php?id=64949

http://www.php.net/ChangeLog-5.php#5.4.17

### Solution

Apply the vendor patch or upgrade to PHP version 5.4.17 or later.

### Risk Factor

High

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2013/07/12, Modified: 2024/05/28

### Plugin Output

tcp/80/www

## 69401 - PHP 5.4.x < 5.4.19 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.19. It is, therefore, potentially affected by the following vulnerabilities :

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

- An error exists related to certificate validation, the 'subjectAltName' field and certificates containing NULL bytes. This error can allow spoofing attacks.

(CVE-2013-4248)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

### See Also

https://bugs.php.net/bug.php?id=65236

http://www.php.net/ChangeLog-5.php#5.4.18

### Solution

Upgrade to PHP version 5.4.19 or later.

Note the 5.4.18 release contains an uninitialized memory read bug and a compile error that prevent proper operation.

### Risk Factor

Medium

### 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

5.9

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

| | |
|---|---|
| BID | 61128 |
| BID | 61776 |
| CVE | CVE-2013-4113 |
| CVE | CVE-2013-4248 |

Plugin Information

Published: 2013/08/21, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 71427 - PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption

### Synopsis

The remote web server uses a version of PHP that is potentially affected by a memory corruption vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.23. It is, therefore, potentially affected by a memory corruption flaw in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter.

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.23

https://seclists.org/fulldisclosure/2013/Dec/96

https://bugzilla.redhat.com/show_bug.cgi?id=1036830

### Solution

Upgrade to PHP version 5.4.23 or later.

### Risk Factor

High

### VPR Score

6.7

### 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 | 64225 |
| CVE | CVE-2013-6420 |

XREF EDB-ID:30395

## Plugin Information

Published: 2013/12/14, Modified: 2024/05/28

## Plugin Output

tcp/80/www

## 73862 - PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation

### Synopsis

The remote web server uses a version of PHP that is potentially affected by a permission escalation vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.28. It is, therefore, potentially affected by a permission escalation vulnerability.

A flaw exists within the FastCGI Process Manager (FPM) when setting permissions for a Unix socket. This could allow a remote attacker to gain elevated privileges after gaining access to the socket.

Note that this plugin has not attempted to exploit this issue, but instead relied only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.28

https://bugs.php.net/bug.php?id=67060

http://www.nessus.org/u?a7b8dfdd

### Solution

Upgrade to PHP version 5.4.28 or later.

### Risk Factor

High

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 67118 |
| CVE | CVE-2014-0185 |

## Plugin Information

Published: 2014/05/05, Modified: 2024/05/28

## Plugin Output

tcp/80/www

## 76281 - PHP 5.4.x < 5.4.30 Multiple Vulnerabilities

### Synopsis

The remote web server is running a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.30. It is, therefore, affected by the following vulnerabilities :

- Boundary checking errors exist related to the Fileinfo extension, Composite Document Format (CDF) handling and the functions 'cdf_read_short_sector', 'cdf_check_stream_offset', 'cdf_count_chain', and 'cdf_read_property_info'. (CVE-2014-0207, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487)

- A pascal string size handling error exists related to the Fileinfo extension and the function 'mconvert'.

(CVE-2014-3478)

- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

- A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

- A type-confusion error exists related to the function 'php_print_info' that could allow disclosure of sensitive information. (CVE-2014-4721)

- An out-of-bounds read error exists in the timelib_meridian_with_check() function due to a failure to properly check string ends. A remote attacker can exploit this to cause a denial of service condition or to disclose memory contents.

- An out-of-bounds read error exists in the date_parse_from_format() function due to a failure in the date parsing routines to properly check string ends. A remote attacker can exploit this to cause a denial of service condition or to disclose memory contents.

- An error exists related to unserialization and 'SplFileObject' handling that could allow denial of service attacks. (Bug #67072)

- A double free error exists related to the Intl extension and the method 'Locale::parseLocale' having unspecified impact. (Bug #67349)

- A buffer overflow error exists related to the Intl extension and the functions 'locale_get_display_name'

and 'uloc_getDisplayName' having unspecified impact.

(Bug #67397)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.30

https://bugs.php.net/bug.php?id=67072
https://bugs.php.net/bug.php?id=67326
https://bugs.php.net/bug.php?id=67349
https://bugs.php.net/bug.php?id=67390
https://bugs.php.net/bug.php?id=67397
https://bugs.php.net/bug.php?id=67410
https://bugs.php.net/bug.php?id=67411
https://bugs.php.net/bug.php?id=67412
https://bugs.php.net/bug.php?id=67413
https://bugs.php.net/bug.php?id=67432
https://bugs.php.net/bug.php?id=67492
https://bugs.php.net/bug.php?id=67498
https://bugs.php.net/bug.php?id=67253
https://bugs.php.net/bug.php?id=67251
https://seclists.org/oss-sec/2014/q3/29
https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html

## Solution

Upgrade to PHP version 5.4.30 or later.

## Risk Factor

High

## VPR Score

5.9

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 67837 |
| BID | 68007 |
| BID | 68120 |
| BID | 68237 |
| BID | 68238 |

| | |
|---|---|
| BID | 68239 |
| BID | 68241 |
| BID | 68243 |
| BID | 68423 |
| BID | 68550 |
| CVE | CVE-2014-0207 |
| CVE | CVE-2014-3478 |
| CVE | CVE-2014-3479 |
| CVE | CVE-2014-3480 |
| CVE | CVE-2014-3487 |
| CVE | CVE-2014-3515 |
| CVE | CVE-2014-3981 |
| CVE | CVE-2014-4049 |
| CVE | CVE-2014-4721 |

## Plugin Information

Published: 2014/06/27, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 78545 - PHP 5.4.x < 5.4.34 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.34. It is, therefore, affected by the following vulnerabilities :

- A buffer overflow error exists in the function 'mkgmtime' that can allow application crashes or arbitrary code execution. (CVE-2014-3668)

- An integer overflow error exists in the function 'unserialize' that can allow denial of service attacks.

Note that this only affects 32-bit instances.

(CVE-2014-3669)

- A heap corruption error exists in the function 'exif_thumbnail' that can allow application crashes or arbitrary code execution. (CVE-2014-3670)

- An input-validation error exists in the cURL extension's file 'ext/curl/interface.c' and NULL option handling that can allow information disclosure. (Bug #68089)

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

### See Also

http://www.php.net/ChangeLog-5.php#5.4.34

### Solution

Upgrade to PHP version 5.4.34 or later.

### Risk Factor

High

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 70611 |
| BID | 70665 |
| BID | 70666 |
| CVE | CVE-2014-3668 |
| CVE | CVE-2014-3669 |
| CVE | CVE-2014-3670 |

Plugin Information

Published: 2014/10/17, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 80330 - PHP 5.4.x < 5.4.36 'process_nested_data' RCE

### Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.36. It is, therefore, affected by a use-after-free error in the 'process_nested_data' function within 'ext/standard/var_unserializer.re' due to improper handling of duplicate keys within the serialized properties of an object. A remote attacker, using a specially crafted call to the 'unserialize' method, can exploit this flaw to execute arbitrary code on the system.

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

### See Also

http://php.net/ChangeLog-5.php#5.4.36

https://bugs.php.net/bug.php?id=68594

http://www.nessus.org/u?88c4ed71

### Solution

Upgrade to PHP version 5.4.36 or later.

### Risk Factor

High

### VPR Score

6.6

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 71791 |
| CVE | CVE-2014-8142 |

## Plugin Information

Published: 2015/01/02, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 81080 - PHP 5.4.x < 5.4.37 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.37. It is, therefore, affected by multiple vulnerabilities:

- The CGI component has an out-of-bounds read flaw in file 'cgi_main.c' when nmap is used to process an invalid file that begins with a hash character (#) but lacks a newline character. A remote attacker, using a specially crafted PHP file, can exploit this vulnerability to disclose memory contents, cause a denial of service, or possibly execute code. (CVE-2014-9427)

- A use-after-free memory error exists in the function 'process_nested_data' within 'var_unserializer.re' due to the improper handling of duplicate numerical keys within the serialized properties of an object. A remote attacker, using a crafted unserialize method call, can exploit this vulnerability to execute arbitrary code.

(CVE-2015-0231)

- A flaw exists in function 'exif_process_unicode' within 'exif.c' that allows freeing an uninitialized pointer. A remote attacker, using specially crafted EXIF data in a JPEG image, can exploit this to cause a denial of service or to execute arbitrary code. (CVE-2015-0232)

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

### See Also

http://php.net/ChangeLog-5.php#5.4.37

https://bugs.php.net/bug.php?id=68618

https://bugs.php.net/bug.php?id=68710

https://bugs.php.net/bug.php?id=68799

### Solution

Upgrade to PHP version 5.4.37 or later.

### 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

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 71833 |
| BID | 72505 |
| BID | 72539 |
| BID | 72541 |
| CVE | CVE-2014-9427 |
| CVE | CVE-2014-9652 |
| CVE | CVE-2015-0231 |
| CVE | CVE-2015-0232 |

Plugin Information

Published: 2015/01/29, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 85298 - PHP 5.4.x < 5.4.44 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP running on the remote web server is 5.4.x prior to 5.4.44. It is, therefore, affected by multiple vulnerabilities:

- Multiple use-after-free vulnerabilities exist in the SPL component, due to improper handling of a specially crafted serialized object. An unauthenticated, remote attack can exploit this, via vectors involving ArrayObject, splObjectStorage and SplDoublyLinkedList to execute arbitrary code. (CVE-2015-6831)

- A use-after-free vulnerability exists in ext/spl/spl_array.c due to improper handling of a specially crafted serialized data. An unauthenticated, remote attacker can exploit this via specially crafted serialized data that triggers misuse of an array field to execute arbitrary code. (CVE-2015-6832)

- A directory traversal vulnerability exists in the PharData class, due to improper implementation of the exctractTo function. An unauthenticated, remote attacker can exploit this via a crafted ZIP archive entry to write to arbitrary files. (CVE-2015-6833)

- The openssl_random_pseudo_bytes() function in file openssl.c does not generate sufficiently random numbers.

An unauthenticated, remote attacker can exploit this to defeat cryptographic protection mechanisms.

(CVE-2015-8867)

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?24db51f6

### Solution

Upgrade to PHP version 5.4.44 or later.

### 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

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 76735 |
| BID | 76737 |
| BID | 76739 |
| BID | 87481 |
| CVE | CVE-2015-6831 |
| CVE | CVE-2015-6832 |
| CVE | CVE-2015-6833 |
| CVE | CVE-2015-8867 |

Plugin Information

Published: 2015/08/11, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 85885 - PHP 5.4.x < 5.4.45 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP running on the remote web server is 5.4.x prior to 5.4.45. It is, therefore, affected by the following vulnerabilities :

- A directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c could allow a remote attacker to create arbitrary empty directories via a crafted ZIP archive.

(CVE-2014-9767)

- Multiple use-after-free memory errors exist related to the unserialize() function. A remote attacker can exploit these errors to execute arbitrary code.

(CVE-2015-6834)

- A use-after-free memory error exists related to the php_var_unserialize() function. A remote attacker, using a crafted serialize string, can exploit this to execute arbitrary code. (CVE-2015-6835)

- A type confusion error exists related to the serialize_function_call() function due to improper validation of the headers field. A remote attacker can exploit this to have unspecified impact. (CVE-2015-6836)

- Multiple flaws exist in the XSLTProcessor class due to improper validation of input from the libxslt library. A remote attacker can exploit thse flaws to have an unspecified impact. (CVE-2015-6837, CVE-2015-6838)

- A flaw exists in the php_zip_extract_file() function in file php_zip.c due to improper sanitization of user-supplied input. An unauthenticated, remote attacker can exploit this to create arbitrary directories outside of the restricted path.

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://php.net/ChangeLog-5.php#5.4.45

### Solution

Upgrade to PHP version 5.4.45 or later.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

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 | 76644 |
| BID | 76649 |
| BID | 76652 |
| BID | 76733 |
| BID | 76734 |
| BID | 76738 |
| CVE | CVE-2014-9767 |
| CVE | CVE-2015-6834 |
| CVE | CVE-2015-6835 |
| CVE | CVE-2015-6836 |
| CVE | CVE-2015-6837 |
| CVE | CVE-2015-6838 |

Plugin Information

Published: 2015/09/10, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 142591 - PHP < 7.3.24 Multiple Vulnerabilities

### Synopsis

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

### Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities

### See Also

https://www.php.net/ChangeLog-7.php#7.3.24

### Solution

Upgrade to PHP version 7.3.24 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### STIG Severity

I

### References

| | |
|---|---|
| XREF | IAVA:2020-A-0510-S |

### Plugin Information

Published: 2020/11/06, Modified: 2024/06/04

### Plugin Output

tcp/80/www

## 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

### Synopsis

The remote service supports the use of medium strength SSL ciphers.

### Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

### See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

### Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### VPR Score

5.1

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

### Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/631/www

## 192219 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6698-1 advisory.

- Vim before 9.0.2142 has a stack-based buffer overflow because did_set_langmap in map.c calls sprintf to write to the error buffer that is passed down to the option callback functions. (CVE-2024-22667)

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

### See Also

https://ubuntu.com/security/notices/USN-6698-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-22667 |
| XREF | USN:6698-1 |

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

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

### Synopsis

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

### Description

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

- A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service. (CVE-2023-52356)

- An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. (CVE-2023-6228)

- An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB.

(CVE-2023-6277)

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

### See Also

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

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-6228 |
| CVE | CVE-2023-6277 |
| CVE | CVE-2023-52356 |
| XREF | USN:6644-1 |

## Plugin Information

Published: 2024/02/19, Modified: 2024/02/19

## Plugin Output

tcp/0

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

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6723-1 advisory.

- Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the KeyTrap issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records. (CVE-2023-50387)

- The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the NSEC3 issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations. (CVE-2023-50868)

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

### See Also

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

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

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

Plugin Information

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

Plugin Output

tcp/0

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

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

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

- An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. (CVE-2024-25062)

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

### See Also

https://ubuntu.com/security/notices/USN-6658-2

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

II

## References

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

## Plugin Information

Published: 2024/03/11, Modified: 2024/03/11

## Plugin Output

tcp/0

## 109650 - Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel vulnerabilities (USN-3641-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3641-1 advisory.

- The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f. (CVE-2018-1000199)

- kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 is vulnerable to a flaw in the way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are delivered once the first instruction after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, potentially, escalate their privileges in the guest. (CVE-2018-1087)

- A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A;

section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.

(CVE-2018-8897)

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

### See Also

https://ubuntu.com/security/notices/USN-3641-1

### Solution

Update the affected kernel package.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.5

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-2018-1000199 |
| CVE | CVE-2018-1087 |
| CVE | CVE-2018-8897 |
| XREF | USN:3641-1 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2018/05/09, Modified: 2024/01/09

Plugin Output

tcp/0

## 99197 - Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel vulnerability (USN-3256-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3256-1 advisory.

- The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls. (CVE-2017-7308)

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

### See Also

https://ubuntu.com/security/notices/USN-3256-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.6

### 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-2017-7308 |
| XREF | USN:3256-1 |

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/04/05, Modified: 2024/01/09

Plugin Output

tcp/0

## 84318 - Ubuntu 14.04 LTS : Linux kernel regression (USN-2643-2)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2643-2 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-2643-2

### Solution

Update the affected kernel package.

### Risk Factor

High

### VPR Score

9.7

### References

| | |
|---|---|
| CVE | CVE-2015-1328 |
| XREF | USN:2643-2 |

### Plugin Information

Published: 2015/06/22, Modified: 2024/01/09

### Plugin Output

tcp/0

## 74214 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2226-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2226-1 advisory.

- drivers/vhost/net.c in the Linux kernel before 3.13.10, when mergeable buffers are disabled, does not properly validate packet lengths, which allows guest OS users to cause a denial of service (memory corruption and host OS crash) or possibly gain privileges on the host OS via crafted packets, related to the handle_rx and get_rx_bufs functions. (CVE-2014-0077)

- The raw_cmd_copyin function in drivers/block/floppy.c in the Linux kernel through 3.14.3 does not properly handle error conditions during processing of an FDRAWCMD ioctl call, which allows local users to trigger kfree operations and gain privileges by leveraging write access to a /dev/fd device. (CVE-2014-1737)

- The raw_cmd_copyout function in drivers/block/floppy.c in the Linux kernel through 3.14.3 does not properly restrict access to certain pointers during processing of an FDRAWCMD ioctl call, which allows local users to obtain sensitive information from kernel heap memory by leveraging write access to a /dev/fd device. (CVE-2014-1738)

- The netback driver in Xen, when using certain Linux versions that do not allow sleeping in softirq context, allows local guest administrators to cause a denial of service (scheduling while atomic error and host crash) via a malformed packet, which causes a mutex to be taken when trying to disable the interface. (CVE-2014-2580)

- Integer overflow in the ping_init_sock function in net/ipv4/ping.c in the Linux kernel through 3.14.1 allows local users to cause a denial of service (use-after-free and system crash) or possibly gain privileges via a crafted application that leverages an improperly managed reference counter.

(CVE-2014-2851)

- The xfs_da3_fixhashpath function in fs/xfs/xfs_da_btree.c in the xfs implementation in the Linux kernel before 3.14.2 does not properly compare btree hash values, which allows local users to cause a denial of service (filesystem corruption, and OOPS or panic) via operations on directories that have hash collisions, as demonstrated by rmdir operations. (CVE-2014-7283)

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

### See Also

https://ubuntu.com/security/notices/USN-2226-1

### Solution

Update the affected kernel package.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 66678 |
| BID | 66779 |
| BID | 67300 |
| BID | 67302 |
| CVE | CVE-2014-0077 |
| CVE | CVE-2014-1737 |
| CVE | CVE-2014-1738 |
| CVE | CVE-2014-2580 |
| CVE | CVE-2014-2851 |
| CVE | CVE-2014-7283 |
| XREF | USN:2226-1 |

Plugin Information

Published: 2014/05/28, Modified: 2024/01/09

Plugin Output

tcp/0

## 77237 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2318-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2318-1 advisory.

- The do_remount function in fs/namespace.c in the Linux kernel through 3.16.1 does not maintain the MNT_LOCK_READONLY bit across a remount of a bind mount, which allows local users to bypass an intended read-only restriction and defeat certain sandbox protection mechanisms via a mount -o remount command within a user namespace. (CVE-2014-5206)

- fs/namespace.c in the Linux kernel through 3.16.1 does not properly restrict clearing MNT_NODEV, MNT_NOSUID, and MNT_NOEXEC and changing MNT_ATIME_MASK during a remount of a bind mount, which allows local users to gain privileges, interfere with backups and auditing on systems that had atime enabled, or cause a denial of service (excessive filesystem updating) on systems that had atime disabled via a mount

-o remount command within a user namespace. (CVE-2014-5207)

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

### See Also

https://ubuntu.com/security/notices/USN-2318-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 69214 |
| BID | 69216 |
| CVE | CVE-2014-5206 |
| CVE | CVE-2014-5207 |
| XREF | USN:2318-1 |

## Plugin Information

Published: 2014/08/18, Modified: 2024/01/09

## Plugin Output

tcp/0

## 77492 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2337-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2337-1 advisory.

- The ioapic_deliver function in virt/kvm/ioapic.c in the Linux kernel through 3.14.1 does not properly validate the kvm_irq_delivery_to_apic return value, which allows guest OS users to cause a denial of service (host OS crash) via a crafted entry in the redirection table of an I/O APIC. NOTE: the affected code was moved to the ioapic_service function before the vulnerability was announced. (CVE-2014-0155)

- The Netlink implementation in the Linux kernel through 3.14.1 does not provide a mechanism for authorizing socket operations based on the opener of a socket, which allows local users to bypass intended access restrictions and modify network configurations by using a Netlink socket for the (1) stdout or (2) stderr of a setuid program. (CVE-2014-0181)

- Array index error in the aio_read_events_ring function in fs/aio.c in the Linux kernel through 3.15.1 allows local users to obtain sensitive information from kernel memory via a large head value.

(CVE-2014-0206)

- The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespaces are inapplicable to inodes, which allows local users to bypass intended chmod restrictions by first creating a user namespace, as demonstrated by setting the setgid bit on a file with group ownership of root. (CVE-2014-4014)

- The rd_build_device_space function in drivers/target/target_core_rd.c in the Linux kernel before 3.14 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from ramdisk_mcp memory by leveraging access to a SCSI initiator. (CVE-2014-4027)

- mm/shmem.c in the Linux kernel through 3.15.1 does not properly implement the interaction between range notification and hole punching, which allows local users to cause a denial of service (i_mutex hold) by using the mmap system call to access a hole, as demonstrated by interfering with intended shmem activity by blocking completion of (1) an MADV_REMOVE madvise call or (2) an FALLOC_FL_PUNCH_HOLE fallocate call.

(CVE-2014-4171)

- arch/x86/kernel/entry_32.S in the Linux kernel through 3.15.1 on 32-bit x86 platforms, when syscall auditing is enabled and the sep CPU feature flag is set, allows local users to cause a denial of service (OOPS and system crash) via an invalid syscall number, as demonstrated by number 1000. (CVE-2014-4508)

- Race condition in the tlv handler functionality in the snd_ctl_elem_user_tlv function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allows local users to obtain sensitive information from kernel memory by leveraging /dev/snd/controlCX access.

(CVE-2014-4652)

- sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not ensure possession of a read/write lock, which allows local users to cause a denial of service (use-after-free) and obtain sensitive information from kernel memory by leveraging /dev/snd/controlCX access.

(CVE-2014-4653)

- The snd_ctl_elem_add function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not check authorization for SNDRV_CTL_IOCTL_ELEM_REPLACE commands, which allows local users to remove kernel controls and cause a denial of service (use-after-free and system crash) by leveraging /dev/snd/controlCX access for an ioctl call. (CVE-2014-4654)

- The snd_ctl_elem_add function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not properly maintain the user_ctl_count value, which allows local users to cause a denial of service (integer overflow and limit bypass) by leveraging /dev/snd/controlCX access for a large number of SNDRV_CTL_IOCTL_ELEM_REPLACE ioctl calls. (CVE-2014-4655)

- Multiple integer overflows in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allow local users to cause a denial of service by leveraging /dev/snd/controlCX access, related to (1) index values in the snd_ctl_add function and (2) numid values in the snd_ctl_remove_numid_conflict function. (CVE-2014-4656)

- The sctp_association_free function in net/sctp/associola.c in the Linux kernel before 3.15.2 does not properly manage a certain backlog value, which allows remote attackers to cause a denial of service (socket outage) via a crafted SCTP packet. (CVE-2014-4667)

- The mountpoint_last function in fs/namei.c in the Linux kernel before 3.15.8 does not properly maintain a certain reference count during attempts to use the umount system call in conjunction with a symlink, which allows local users to cause a denial of service (memory consumption or use-after-free) or possibly have unspecified other impact via the umount program. (CVE-2014-5045)

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

See Also

https://ubuntu.com/security/notices/USN-2337-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 66688 |
| BID | 67034 |
| BID | 67985 |
| BID | 67988 |
| BID | 68126 |
| BID | 68157 |
| BID | 68162 |
| BID | 68163 |
| BID | 68164 |
| BID | 68170 |
| BID | 68176 |
| BID | 68224 |
| BID | 68862 |
| CVE | CVE-2014-0155 |
| CVE | CVE-2014-0181 |
| CVE | CVE-2014-0206 |
| CVE | CVE-2014-4014 |
| CVE | CVE-2014-4027 |
| CVE | CVE-2014-4171 |
| CVE | CVE-2014-4508 |
| CVE | CVE-2014-4652 |
| CVE | CVE-2014-4653 |
| CVE | CVE-2014-4654 |
| CVE | CVE-2014-4655 |
| CVE | CVE-2014-4656 |
| CVE | CVE-2014-4667 |
| CVE | CVE-2014-5045 |
| XREF | USN:2337-1 |

## Plugin Information

Published: 2014/09/03, Modified: 2024/01/09

## Plugin Output

tcp/0

## 77821 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2359-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2359-1 advisory.

- The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.16.1 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to (1) cause a denial of service (host OS memory corruption) or possibly have unspecified other impact by triggering a large gfn value or (2) cause a denial of service (host OS memory consumption) by triggering a small gfn value that leads to permanently pinned pages. (CVE-2014-3601)

- The sctp_assoc_update function in net/sctp/associola.c in the Linux kernel through 3.15.8, when SCTP authentication is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by starting to establish an association between two endpoints immediately after an exchange of INIT and INIT ACK chunks to establish an earlier association between these endpoints in the opposite direction. (CVE-2014-5077)

- Stack consumption vulnerability in the parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (uncontrolled recursion, and system crash or reboot) via a crafted iso9660 image with a CL entry referring to a directory entry that has a CL entry. (CVE-2014-5471)

- The parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (unkillable mount process) via a crafted iso9660 image with a self-referential CL entry. (CVE-2014-5472)

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

### See Also

https://ubuntu.com/security/notices/USN-2359-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 68881 |
| BID | 69396 |
| BID | 69428 |
| BID | 69489 |
| CVE | CVE-2014-3601 |
| CVE | CVE-2014-5077 |
| CVE | CVE-2014-5471 |
| CVE | CVE-2014-5472 |
| XREF | USN:2359-1 |

Plugin Information

Published: 2014/09/24, Modified: 2024/01/09

Plugin Output

tcp/0

## 78259 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2379-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2379-1 advisory.

- Multiple stack-based buffer overflows in the magicmouse_raw_event function in drivers/hid/hid-magicmouse.c in the Magic Mouse HID driver in the Linux kernel through 3.16.3 allow physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with an event. (CVE-2014-3181)

- The report_fixup functions in the HID subsystem in the Linux kernel before 3.16.2 might allow physically proximate attackers to cause a denial of service (out-of-bounds write) via a crafted device that provides a small report descriptor, related to (1) drivers/hid/hid-cherry.c, (2) drivers/hid/hid-kye.c, (3) drivers/hid/hid-lg.c, (4) drivers/hid/hid-monterey.c, (5) drivers/hid/hid-petalynx.c, and (6) drivers/hid/hid-sunplus.c. (CVE-2014-3184)

- Multiple buffer overflows in the command_port_read_callback function in drivers/usb/serial/whiteheat.c in the Whiteheat USB Serial Driver in the Linux kernel before 3.16.2 allow physically proximate attackers to execute arbitrary code or cause a denial of service (memory corruption and system crash) via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with a bulk response.

(CVE-2014-3185)

- Buffer overflow in the picolcd_raw_event function in devices/hid/hid-picolcd_core.c in the PicoLCD HID device driver in the Linux kernel through 3.16.3, as used in Android on Nexus 7 devices, allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted device that sends a large report. (CVE-2014-3186)

- The assoc_array_gc function in the associative-array implementation in lib/assoc_array.c in the Linux kernel before 3.16.3 does not properly implement garbage collection, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via multiple keyctl newring operations followed by a keyctl timeout operation. (CVE-2014-3631)

- The __udf_read_inode function in fs/udf/inode.c in the Linux kernel through 3.16.3 does not restrict the amount of ICB indirection, which allows physically proximate attackers to cause a denial of service (infinite loop or stack consumption) via a UDF filesystem with a crafted inode. (CVE-2014-6410)

- Buffer overflow in net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, allows remote attackers to cause a denial of service (memory corruption and panic) or possibly have unspecified other impact via a long unencrypted auth ticket. (CVE-2014-6416)

- net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, does not properly consider the possibility of kmalloc failure, which allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a long unencrypted auth ticket. (CVE-2014-6417)

- net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, does not properly validate auth replies, which allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via crafted data from the IP address of a Ceph Monitor. (CVE-2014-6418)

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

## See Also

https://ubuntu.com/security/notices/USN-2379-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 69763 |
| BID | 69768 |
| BID | 69779 |
| BID | 69781 |
| BID | 69799 |
| BID | 69805 |
| BID | 70095 |
| CVE | CVE-2014-3181 |
| CVE | CVE-2014-3184 |
| CVE | CVE-2014-3185 |
| CVE | CVE-2014-3186 |

| | |
|---|---|
| CVE | CVE-2014-3631 |
| CVE | CVE-2014-6410 |
| CVE | CVE-2014-6416 |
| CVE | CVE-2014-6417 |
| CVE | CVE-2014-6418 |
| XREF | USN:2379-1 |

## Plugin Information

Published: 2014/10/11, Modified: 2024/01/09

## Plugin Output

tcp/0

## 80032 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2446-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2446-1 advisory.

- The SCTP implementation in the Linux kernel through 3.17.2 allows remote attackers to cause a denial of service (system crash) via a malformed ASCONF chunk, related to net/sctp/sm_make_chunk.c and net/sctp/sm_statefuns.c. (CVE-2014-3673)

- The sctp_assoc_lookup_asconf_ack function in net/sctp/associola.c in the SCTP implementation in the Linux kernel through 3.17.2 allows remote attackers to cause a denial of service (panic) via duplicate ASCONF chunks that trigger an incorrect uncork within the side-effect interpreter. (CVE-2014-3687)

- The SCTP implementation in the Linux kernel before 3.17.4 allows remote attackers to cause a denial of service (memory consumption) by triggering a large number of chunks in an association's output queue, as demonstrated by ASCONF probes, related to net/sctp/inqueue.c and net/sctp/sm_statefuns.c. (CVE-2014-3688)

- kernel/trace/trace_syscalls.c in the Linux kernel through 3.17.2 does not properly handle private syscall numbers during use of the perf subsystem, which allows local users to cause a denial of service (out-of- bounds read and OOPS) or bypass the ASLR protection mechanism via a crafted application. (CVE-2014-7825)

- kernel/trace/trace_syscalls.c in the Linux kernel through 3.17.2 does not properly handle private syscall numbers during use of the ftrace subsystem, which allows local users to gain privileges or cause a denial of service (invalid pointer dereference) via a crafted application. (CVE-2014-7826)

- The paravirt_ops_setup function in arch/x86/kernel/kvm.c in the Linux kernel through 3.18 uses an improper paravirt_enabled setting for KVM guest kernels, which makes it easier for guest OS users to bypass the ASLR protection mechanism via a crafted application that reads a 16-bit value. (CVE-2014-8134)

- The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.17.2 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to cause a denial of service (host OS page unpinning) or possibly have unspecified other impact by leveraging guest OS privileges. NOTE: this vulnerability exists because of an incorrect fix for CVE-2014-3601. (CVE-2014-8369)

- The do_double_fault function in arch/x86/kernel/traps.c in the Linux kernel through 3.17.4 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to cause a denial of service (panic) via a modify_ldt system call, as demonstrated by sigreturn_32 in the linux-clock-tests test suite. (CVE-2014-9090)

- arch/x86/kernel/entry_64.S in the Linux kernel before 3.17.5 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to gain privileges by triggering an IRET instruction that leads to access to a GS Base address from the wrong space. (CVE-2014-9322)

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

## See Also

https://ubuntu.com/security/notices/USN-2446-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

8.4

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 70749 |
| BID | 70766 |
| BID | 70768 |
| BID | 70883 |
| BID | 70971 |
| BID | 70972 |
| BID | 71250 |
| CVE | CVE-2014-3673 |
| CVE | CVE-2014-3687 |
| CVE | CVE-2014-3688 |
| CVE | CVE-2014-7825 |
| CVE | CVE-2014-7826 |
| CVE | CVE-2014-8134 |

| | |
|---|---|
| CVE | CVE-2014-8369 |
| CVE | CVE-2014-9090 |
| CVE | CVE-2014-9322 |
| XREF | USN:2446-1 |

## Plugin Information

Published: 2014/12/15, Modified: 2024/01/09

## Plugin Output

tcp/0

## 80513 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2466-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2466-1 advisory.

- The sctp_process_param function in net/sctp/sm_make_chunk.c in the SCTP implementation in the Linux kernel before 3.17.4, when ASCONF is used, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via a malformed INIT chunk. (CVE-2014-7841)

- Race condition in arch/x86/kvm/x86.c in the Linux kernel before 3.17.4 allows guest OS users to cause a denial of service (guest OS crash) via a crafted application that performs an MMIO transaction or a PIO transaction to trigger a guest userspace emulation error report, a similar issue to CVE-2010-5313.

(CVE-2014-7842)

- The __clear_user function in arch/arm64/lib/clear_user.S in the Linux kernel before 3.17.4 on the ARM64 platform allows local users to cause a denial of service (system crash) by reading one byte beyond a /dev/zero page boundary. (CVE-2014-7843)

- Stack-based buffer overflow in the ttusbdecfe_dvbs_diseqc_send_master_cmd function in drivers/media/usb/ttusb-dec/ttusbdecfe.c in the Linux kernel before 3.17.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via a large message length in an ioctl call.

(CVE-2014-8884)

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

### See Also

https://ubuntu.com/security/notices/USN-2466-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 71078 |
| BID | 71081 |
| BID | 71082 |
| BID | 71097 |
| CVE | CVE-2014-7841 |
| CVE | CVE-2014-7842 |
| CVE | CVE-2014-7843 |
| CVE | CVE-2014-8884 |
| XREF | USN:2466-1 |

Plugin Information

Published: 2015/01/14, Modified: 2024/01/09

Plugin Output

tcp/0

## 82071 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2544-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2544-1 advisory.

- The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a module name in the salg_name field, a different vulnerability than CVE-2014-9644. (CVE-2013-7421)

- The implementation of certain splice_write file operations in the Linux kernel before 3.16 does not enforce a restriction on the maximum size of a single file, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted splice system call, as demonstrated by use of a file descriptor associated with an ext4 filesystem. (CVE-2014-7822)

- The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a parenthesized module template expression in the salg_name field, as demonstrated by the vfat(aes) expression, a different vulnerability than CVE-2013-7421.

(CVE-2014-9644)

- The UDF filesystem implementation in the Linux kernel before 3.18.2 does not validate certain lengths, which allows local users to cause a denial of service (buffer over-read and system crash) via a crafted filesystem image, related to fs/udf/inode.c and fs/udf/symlink.c. (CVE-2014-9728)

- The udf_read_inode function in fs/udf/inode.c in the Linux kernel before 3.18.2 does not ensure a certain data-structure size consistency, which allows local users to cause a denial of service (system crash) via a crafted UDF filesystem image. (CVE-2014-9729)

- The udf_pc_to_char function in fs/udf/symlink.c in the Linux kernel before 3.18.2 relies on component lengths that are unused, which allows local users to cause a denial of service (system crash) via a crafted UDF filesystem image. (CVE-2014-9730)

- The UDF filesystem implementation in the Linux kernel before 3.18.2 does not ensure that space is available for storing a symlink target's name along with a trailing \0 character, which allows local users to obtain sensitive information via a crafted filesystem image, related to fs/udf/symlink.c and fs/udf/unicode.c. (CVE-2014-9731)

- The XFS implementation in the Linux kernel before 3.15 improperly uses an old size value during remote attribute replacement, which allows local users to cause a denial of service (transaction overrun and data corruption) or possibly gain privileges by leveraging XFS filesystem access. (CVE-2015-0274)

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

### See Also

https://ubuntu.com/security/notices/USN-2544-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.0

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 72320 |
| BID | 72322 |
| BID | 73156 |
| CVE | CVE-2013-7421 |
| CVE | CVE-2014-7822 |
| CVE | CVE-2014-9644 |
| CVE | CVE-2014-9728 |
| CVE | CVE-2014-9729 |
| CVE | CVE-2014-9730 |
| CVE | CVE-2014-9731 |
| CVE | CVE-2015-0274 |
| XREF | USN:2544-1 |

## Plugin Information

Published: 2015/03/25, Modified: 2024/01/09

Plugin Output

tcp/0

## 82662 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2563-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2563-1 advisory.

- Use-after-free vulnerability in the sctp_assoc_update function in net/sctp/associola.c in the Linux kernel before 3.18.8 allows remote attackers to cause a denial of service (slab corruption and panic) or possibly have unspecified other impact by triggering an INIT collision that leads to improper handling of shared- key data. (CVE-2015-1421)

- The IPv4 implementation in the Linux kernel before 3.18.8 does not properly consider the length of the Read-Copy Update (RCU) grace period for redirecting lookups in the absence of caching, which allows remote attackers to cause a denial of service (memory consumption or system crash) via a flood of packets. (CVE-2015-1465)

- The stack randomization feature in the Linux kernel before 3.19.1 on 64-bit platforms uses incorrect data types for the results of bitwise left-shift operations, which makes it easier for attackers to bypass the ASLR protection mechanism by predicting the address of the top of the stack, related to the randomize_stack_top function in fs/binfmt_elf.c and the stack_maxrandom_size function in arch/x86/mm/mmap.c. (CVE-2015-1593)

- net/llc/sysctl_net_llc.c in the Linux kernel before 3.19 uses an incorrect data type in a sysctl table, which allows local users to obtain potentially sensitive information from kernel memory or possibly have unspecified other impact by accessing a sysctl entry. (CVE-2015-2041)

- net/rds/sysctl.c in the Linux kernel before 3.19 uses an incorrect data type in a sysctl table, which allows local users to obtain potentially sensitive information from kernel memory or possibly have unspecified other impact by accessing a sysctl entry. (CVE-2015-2042)

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

### See Also

https://ubuntu.com/security/notices/USN-2563-1

### Solution

Update the affected kernel package.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

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 | 72356 |
| BID | 72435 |
| CVE | CVE-2015-1421 |
| CVE | CVE-2015-1465 |
| CVE | CVE-2015-1593 |
| CVE | CVE-2015-2041 |
| CVE | CVE-2015-2042 |
| XREF | USN:2563-1 |

Plugin Information

Published: 2015/04/09, Modified: 2024/01/09

Plugin Output

tcp/0

## 83179 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2588-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2588-1 advisory.

- Stack-based buffer overflow in the get_matching_model_microcode function in arch/x86/kernel/cpu/microcode/intel_early.c in the Linux kernel before 4.0 allows context-dependent attackers to gain privileges by constructing a crafted microcode header and leveraging root privileges for write access to the initrd. (CVE-2015-2666)

- The ndisc_router_discovery function in net/ipv6/ndisc.c in the Neighbor Discovery (ND) protocol implementation in the IPv6 stack in the Linux kernel before 3.19.6 allows remote attackers to reconfigure a hop-limit setting via a small hop_limit value in a Router Advertisement (RA) message. (CVE-2015-2922)

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

### See Also

https://ubuntu.com/security/notices/USN-2588-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 73183 |
| BID | 74315 |
| CVE | CVE-2015-2666 |
| CVE | CVE-2015-2922 |
| XREF | USN:2588-1 |

## Plugin Information

Published: 2015/05/01, Modified: 2024/01/09

## Plugin Output

tcp/0

## 84121 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2634-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2634-1 advisory.

- The ping_unhash function in net/ipv4/ping.c in the Linux kernel before 4.0.3 does not initialize a certain list data structure during an unhash operation, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) by leveraging the ability to make a SOCK_DGRAM socket system call for the IPPROTO_ICMP or IPPROTO_ICMPV6 protocol, and then making a connect system call after a disconnect. (CVE-2015-3636)

- Array index error in the tcm_vhost_make_tpg function in drivers/vhost/scsi.c in the Linux kernel before 4.0 might allow guest OS users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted VHOST_SCSI_SET_ENDPOINT ioctl call. NOTE: the affected function was renamed to vhost_scsi_make_tpg before the vulnerability was announced. (CVE-2015-4036)

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

### See Also

https://ubuntu.com/security/notices/USN-2634-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-3636 |
| CVE | CVE-2015-4036 |
| XREF | USN:2634-1 |

Plugin Information

Published: 2015/06/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 84982 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2681-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2681-1 advisory.

- The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an I/O vector array overrun. (CVE-2015-1805)

- The kvm_apic_has_events function in arch/x86/kvm/lapic.h in the Linux kernel through 4.1.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging /dev/kvm access for an ioctl call. (CVE-2015-4692)

- The bpf_int_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel before 4.0.6 allows local users to cause a denial of service (system crash) by creating a packet filter and then loading crafted BPF instructions that trigger late convergence by the JIT compiler. (CVE-2015-4700)

- The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 do not properly consider yielding a processor, which allows remote attackers to cause a denial of service (system hang) via incorrect checksums within a UDP packet flood. (CVE-2015-5364)

- The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 provide inappropriate

-EAGAIN return values, which allows remote attackers to cause a denial of service (EPOLLET epoll application read outage) via an incorrect checksum in a UDP packet, a different vulnerability than CVE-2015-5364. (CVE-2015-5366)

- Use-after-free vulnerability in the path_openat function in fs/namei.c in the Linux kernel 3.x and 4.x before 4.0.4 allows local users to cause a denial of service or possibly have unspecified other impact via O_TMPFILE filesystem operations that leverage a duplicate cleanup operation. (CVE-2015-5706)

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

### See Also

https://ubuntu.com/security/notices/USN-2681-1

### Solution

Update the affected kernel package.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.2

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

| | |
|---|---|
| BID | 74951 |
| CVE | CVE-2015-1805 |
| CVE | CVE-2015-4692 |
| CVE | CVE-2015-4700 |
| CVE | CVE-2015-5364 |
| CVE | CVE-2015-5366 |
| CVE | CVE-2015-5706 |
| XREF | USN:2681-1 |

Plugin Information

Published: 2015/07/24, Modified: 2024/01/09

Plugin Output

tcp/0

## 85076 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2688-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2688-1 advisory.

- Memory leak in the __key_link_end function in security/keys/keyring.c in the Linux kernel before 4.1.4 allows local users to cause a denial of service (memory consumption) via many add_key system calls that refer to existing keys. (CVE-2015-1333)

- arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform improperly relies on espfix64 during nested NMI processing, which allows local users to gain privileges by triggering an NMI within a certain instruction window. (CVE-2015-3290)

- arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform does not properly determine when nested NMI processing is occurring, which allows local users to cause a denial of service (skipped NMI) by modifying the rsp register, issuing a syscall instruction, and triggering an NMI.

(CVE-2015-3291)

- arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform mishandles IRET faults in processing NMIs that occurred during userspace execution, which might allow local users to gain privileges by triggering an NMI. (CVE-2015-5157)

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

### See Also

https://ubuntu.com/security/notices/USN-2688-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-1333 |
| CVE | CVE-2015-3290 |
| CVE | CVE-2015-3291 |
| CVE | CVE-2015-5157 |
| XREF | USN:2688-1 |

Plugin Information

Published: 2015/07/29, Modified: 2024/01/09

Plugin Output

tcp/0

## 85158 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2700-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2700-1 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-2700-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### VPR Score

6.7

### References

| | |
|---|---|
| CVE | CVE-2015-3290 |
| CVE | CVE-2015-3291 |
| CVE | CVE-2015-5157 |
| XREF | USN:2700-1 |

### Plugin Information

Published: 2015/07/31, Modified: 2024/01/09

### Plugin Output

tcp/0

## 86467 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2776-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2776-1 advisory.

- GNOME NetworkManager allows remote attackers to cause a denial of service (IPv6 traffic disruption) via a crafted MTU value in an IPv6 Router Advertisement (RA) message, a different vulnerability than CVE-2015-8215. (CVE-2015-0272)

- The virtnet_probe function in drivers/net/virtio_net.c in the Linux kernel before 4.2 attempts to support a FRAGLIST feature without proper memory allocation, which allows guest OS users to cause a denial of service (buffer overflow and memory corruption) via a crafted sequence of fragmented packets.

(CVE-2015-5156)

- The __rds_conn_create function in net/rds/connection.c in the Linux kernel through 4.2.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound. (CVE-2015-6937)

- Multiple race conditions in the Advanced Union Filesystem (aufs) aufs3-mmap.patch and aufs4-mmap.patch patches for the Linux kernel 3.x and 4.x allow local users to cause a denial of service (use-after-free and BUG) or possibly gain privileges via a (1) madvise or (2) msync system call, related to mm/madvise.c and mm/msync.c. (CVE-2015-7312)

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

### See Also

https://ubuntu.com/security/notices/USN-2776-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-0272 |
| CVE | CVE-2015-5156 |
| CVE | CVE-2015-6937 |
| CVE | CVE-2015-7312 |
| XREF | USN:2776-1 |

Plugin Information

Published: 2015/10/20, Modified: 2024/01/09

Plugin Output

tcp/0

## 87531 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2848-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2848-1 advisory.

- Xen, when used on a system providing PV backends, allows local guest OS administrators to cause a denial of service (host OS crash) or gain privileges by writing to memory shared between the frontend and backend, aka a double fetch vulnerability. (CVE-2015-8550)

- The PCI backend driver in Xen, when running on an x86 system and using Linux 3.1.x through 4.3.x as the driver domain, allows local guest administrators to hit BUG conditions and cause a denial of service (NULL pointer dereference and host OS crash) by leveraging a system with access to a passed-through MSI or MSI-X capable physical PCI device and a crafted sequence of XEN_PCI_OP_* operations, aka Linux pciback missing sanity checks. (CVE-2015-8551)

- The PCI backend driver in Xen, when running on an x86 system and using Linux 3.1.x through 4.3.x as the driver domain, allows local guest administrators to generate a continuous stream of WARN messages and cause a denial of service (disk consumption) by leveraging a system with access to a passed-through MSI or MSI-X capable physical PCI device and XEN_PCI_OP_enable_msi operations, aka Linux pciback missing sanity checks. (CVE-2015-8552)

- kernel/ptrace.c in the Linux kernel through 4.4.1 mishandles uid and gid mappings, which allows local users to gain privileges by establishing a user namespace, waiting for a root process to enter that namespace with an unsafe uid or gid, and then using the ptrace system call. NOTE: the vendor states there is no kernel bug here. (CVE-2015-8709)

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

### See Also

https://ubuntu.com/security/notices/USN-2848-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-8550 |
| CVE | CVE-2015-8551 |
| CVE | CVE-2015-8552 |
| CVE | CVE-2015-8709 |
| XREF | USN:2848-1 |

Plugin Information

Published: 2015/12/21, Modified: 2024/01/09

Plugin Output

tcp/0

## 88895 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2907-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2907-1 advisory.

- The keyctl_read_key function in security/keys/keyctl.c in the Linux kernel before 4.3.4 does not properly use a semaphore, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted application that leverages a race condition between keyctl_revoke and keyctl_read calls. (CVE-2015-7550)

- The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application. (CVE-2015-8543)

- The (1) pptp_bind and (2) pptp_connect functions in drivers/net/ppp/pptp.c in the Linux kernel through 4.3.3 do not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application. (CVE-2015-8569)

- The sco_sock_bind function in net/bluetooth/sco.c in the Linux kernel before 4.3.4 does not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application. (CVE-2015-8575)

- The fuse_fill_write_pages function in fs/fuse/file.c in the Linux kernel before 4.4 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers a zero length for the first segment of an iov. (CVE-2015-8785)

- The overlayfs implementation in the Linux kernel through 4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.

(CVE-2016-1575)

- The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program. (CVE-2016-1576)

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

### See Also

https://ubuntu.com/security/notices/USN-2907-1

### Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-7550 |
| CVE | CVE-2015-8543 |
| CVE | CVE-2015-8569 |
| CVE | CVE-2015-8575 |
| CVE | CVE-2015-8785 |
| CVE | CVE-2016-1575 |
| CVE | CVE-2016-1576 |
| XREF | USN:2907-1 |

Plugin Information

Published: 2016/02/23, Modified: 2024/01/09

Plugin Output

tcp/0

## 89932 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2929-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2929-1 advisory.

- The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garbage.c. (CVE-2013-4312)

- The clie_5_attach function in drivers/usb/serial/visor.c in the Linux kernel through 4.4.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a bulk-out endpoint.

(CVE-2015-7566)

- The usbvision driver in the Linux kernel package 3.10.0-123.20.1.el7 through 3.10.0-229.14.1.el7 in Red Hat Enterprise Linux (RHEL) 7.1 allows physically proximate attackers to cause a denial of service (panic) via a nonzero bInterfaceNumber value in a USB device descriptor. (CVE-2015-7833)

- Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linux kernel through 4.4.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after- free and system crash) by making a TIOCGETD ioctl call during processing of a TIOCSETD ioctl call.

(CVE-2016-0723)

- Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor. (CVE-2016-2384)

- The snd_seq_ioctl_remove_events function in sound/core/seq/seq_clientmgr.c in the Linux kernel before 4.4.1 does not verify FIFO assignment before proceeding with FIFO clearing, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted ioctl call. (CVE-2016-2543)

- Race condition in the queue_delete function in sound/core/seq/seq_queue.c in the Linux kernel before 4.4.1 allows local users to cause a denial of service (use-after-free and system crash) by making an ioctl call at a certain time. (CVE-2016-2544)

- The snd_timer_interrupt function in sound/core/timer.c in the Linux kernel before 4.4.1 does not properly maintain a certain linked list, which allows local users to cause a denial of service (race condition and system crash) via a crafted ioctl call. (CVE-2016-2545)

- sound/core/timer.c in the Linux kernel before 4.4.1 uses an incorrect type of mutex, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call. (CVE-2016-2546)

- sound/core/timer.c in the Linux kernel before 4.4.1 employs a locking approach that does not consider slave timer instances, which allows local users to cause a denial of service (race condition, use-after- free, and system crash) via a crafted ioctl call. (CVE-2016-2547)

- sound/core/timer.c in the Linux kernel before 4.4.1 retains certain linked lists after a close or stop action, which allows local users to cause a denial of service (system crash) via a crafted ioctl call, related to the (1) snd_timer_close and (2) _snd_timer_stop functions. (CVE-2016-2548)

- sound/core/hrtimer.c in the Linux kernel before 4.4.1 does not prevent recursive callback access, which allows local users to cause a denial of service (deadlock) via a crafted ioctl call. (CVE-2016-2549)

- The treo_attach function in drivers/usb/serial/visor.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a (1) bulk-in or (2) interrupt-in endpoint. (CVE-2016-2782)

- The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call. (CVE-2016-3134)

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

## See Also

https://ubuntu.com/security/notices/USN-2929-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.9

## 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-2013-4312 |
| CVE | CVE-2015-7566 |
| CVE | CVE-2015-7833 |
| CVE | CVE-2016-0723 |
| CVE | CVE-2016-2384 |
| CVE | CVE-2016-2543 |
| CVE | CVE-2016-2544 |
| CVE | CVE-2016-2545 |
| CVE | CVE-2016-2546 |
| CVE | CVE-2016-2547 |
| CVE | CVE-2016-2548 |
| CVE | CVE-2016-2549 |
| CVE | CVE-2016-2782 |
| CVE | CVE-2016-3134 |
| XREF | USN:2929-1 |

## Plugin Information

Published: 2016/03/15, Modified: 2024/01/09

## Plugin Output

tcp/0

## 91088 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2968-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2968-1 advisory.

- The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device that lacks endpoints. (CVE-2015-7515)

- Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE:

this vulnerability exists because of a CVE-2012-6701 regression. (CVE-2015-8830)

- The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in a certain Linux kernel backport in the linux package before 3.2.73-2+deb7u3 on Debian wheezy and the kernel package before 3.10.0-229.26.2 on Red Hat Enterprise Linux (RHEL) 7.1 do not properly consider the side effects of failed

__copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an I/O vector array overrun. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-1805. (CVE-2016-0774)

- The LIST_POISON feature in include/linux/poison.h in the Linux kernel before 4.3, as used in Android 6.0.1 before 2016-03-01, does not properly consider the relationship to the mmap_min_addr value, which makes it easier for attackers to bypass a poison-pointer protection mechanism by triggering the use of an uninitialized list entry, aka Android internal bug 26186802, a different vulnerability than CVE-2015-3636.

(CVE-2016-0821)

- The create_fixed_stream_quirk function in sound/usb/quirks.c in the snd-usb-audio driver in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference or double free, and system crash) via a crafted endpoints value in a USB device descriptor.

(CVE-2016-2184)

- The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. (CVE-2016-2185)

- The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. (CVE-2016-2186)

- The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. (CVE-2016-2188)

- The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors. (CVE-2016-3136)

- drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both an interrupt-in and an interrupt-out endpoint descriptor, related to the cypress_generic_port_probe and cypress_open functions. (CVE-2016-3137)

- The acm_probe function in drivers/usb/class/cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both a control and a data endpoint descriptor. (CVE-2016-3138)

- The digi_port_init function in drivers/usb/serial/digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. (CVE-2016-3140)

- The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses. (CVE-2016-3156)

- The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows local guest OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by leveraging I/O port access.

(CVE-2016-3157)

- The ims_pcu_parse_cdc_data function in drivers/input/misc/ims-pcu.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (system crash) via a USB device without both a master and a slave interface. (CVE-2016-3689)

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

## See Also

https://ubuntu.com/security/notices/USN-2968-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

5.9

## 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-2015-7515 |
| CVE | CVE-2015-8830 |
| CVE | CVE-2016-0774 |
| CVE | CVE-2016-0821 |
| CVE | CVE-2016-2184 |
| CVE | CVE-2016-2185 |
| CVE | CVE-2016-2186 |
| CVE | CVE-2016-2188 |
| CVE | CVE-2016-3136 |
| CVE | CVE-2016-3137 |
| CVE | CVE-2016-3138 |
| CVE | CVE-2016-3140 |
| CVE | CVE-2016-3156 |
| CVE | CVE-2016-3157 |
| CVE | CVE-2016-3689 |
| XREF | USN:2968-1 |

## Plugin Information

Published: 2016/05/12, Modified: 2024/01/09

## Plugin Output

tcp/0

## 91880 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3018-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3018-1 advisory.

- The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted USBDEVFS_CONNECTINFO ioctl call. (CVE-2016-4482)

- The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface. (CVE-2016-4565)

- The snd_timer_user_params function in sound/core/timer.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface. (CVE-2016-4569)

- sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.

(CVE-2016-4578)

- The x25_negotiate_facilities function in net/x25/x25_facilities.c in the Linux kernel before 4.5.5 does not properly initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory via an X.25 Call Request. (CVE-2016-4580)

- The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.

(CVE-2016-4913)

- The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement. (CVE-2016-4997)

- The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from kernel heap memory by leveraging in-container root access to provide a crafted offset value that leads to crossing a ruleset blob boundary. (CVE-2016-4998)

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

### See Also

https://ubuntu.com/security/notices/USN-3018-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

9.0

## 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-2016-4482 |
| CVE | CVE-2016-4565 |
| CVE | CVE-2016-4569 |
| CVE | CVE-2016-4578 |
| CVE | CVE-2016-4580 |
| CVE | CVE-2016-4913 |
| CVE | CVE-2016-4997 |
| CVE | CVE-2016-4998 |
| XREF | USN:3018-1 |

## Exploitable With

Metasploit (true)

## Plugin Information

Published: 2016/06/28, Modified: 2024/01/09

Plugin Output

tcp/0

## 93218 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3071-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3071-1 advisory.

- The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from kernel stack memory by reading an RDS message. (CVE-2016-5244)

- net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.

(CVE-2016-5696)

- Race condition in the vop_ioctl function in drivers/misc/mic/vop/vop_vringh.c in the MIC VOP driver in the Linux kernel before 4.6.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (memory corruption and system crash) by changing a certain header, aka a double fetch vulnerability. (CVE-2016-5728)

- The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call. (CVE-2016-5828)

- Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call. (CVE-2016-5829)

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

### See Also

https://ubuntu.com/security/notices/USN-3071-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-5244 |
| CVE | CVE-2016-5696 |
| CVE | CVE-2016-5728 |
| CVE | CVE-2016-5828 |
| CVE | CVE-2016-5829 |
| XREF | USN:3071-1 |

Plugin Information

Published: 2016/08/30, Modified: 2024/01/09

Plugin Output

tcp/0

## 93602 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3083-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3083-1 advisory.

- net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call. (CVE-2015-8767)

- The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendmsg system call. (CVE-2016-3841)

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

### See Also

https://ubuntu.com/security/notices/USN-3083-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-8767 |
| CVE | CVE-2016-3841 |
| XREF | USN:3083-1 |

Plugin Information

Published: 2016/09/20, Modified: 2024/01/09

Plugin Output

tcp/0

## 94731 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3127-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3127-1 advisory.

- The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call. (CVE-2014-9904)

- mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero. (CVE-2015-3288)

- Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest OS users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area. (CVE-2016-3961)

- The proc_keys_show function in security/keys/proc.c in the Linux kernel through 4.8.2, when the GNU Compiler Collection (gcc) stack protector is enabled, uses an incorrect buffer size for certain timeout data, which allows local users to cause a denial of service (stack memory corruption and panic) by reading the /proc/keys file. (CVE-2016-7042)

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

### See Also

https://ubuntu.com/security/notices/USN-3127-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2014-9904 |
| CVE | CVE-2015-3288 |
| CVE | CVE-2016-3961 |
| CVE | CVE-2016-7042 |
| XREF | USN:3127-1 |

Plugin Information

Published: 2016/11/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 95430 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3145-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3145-1 advisory.

- The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code. (CVE-2016-7425)

- Stack-based buffer overflow in the brcmf_cfg80211_start_ap function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.7.5 allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a long SSID Information Element in a command to a Netlink socket. (CVE-2016-8658)

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

### See Also

https://ubuntu.com/security/notices/USN-3145-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-7425 |
| CVE | CVE-2016-8658 |
| XREF | USN:3145-1 |

Plugin Information

Published: 2016/12/01, Modified: 2024/01/09

Plugin Output

tcp/0

## 96437 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3168-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3168-1 advisory.

- arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application. (CVE-2016-9756)

- The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.

(CVE-2016-9793)

- Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command. (CVE-2016-9794)

- Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated. (CVE-2016-9806)

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

### See Also

https://ubuntu.com/security/notices/USN-3168-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-9756 |
| CVE | CVE-2016-9793 |
| CVE | CVE-2016-9794 |
| CVE | CVE-2016-9806 |
| XREF | USN:3168-1 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2017/01/12, Modified: 2024/01/09

Plugin Output

tcp/0

## 97320 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3207-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3207-1 advisory.

- Use-after-free vulnerability in the disk_seqf_stop function in block/genhd.c in the Linux kernel before 4.7.1 allows local users to gain privileges by leveraging the execution of a certain stop operation even if the corresponding start operation had failed. (CVE-2016-7910)

- Race condition in the get_task_ioprio function in block/ioprio.c in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted ioprio_get system call. (CVE-2016-7911)

- The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call. (CVE-2017-6074)

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

### See Also

https://ubuntu.com/security/notices/USN-3207-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.0

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

| | |
|---|---|
| CVE | CVE-2016-7910 |
| CVE | CVE-2016-7911 |
| CVE | CVE-2017-6074 |
| XREF | USN:3207-1 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2017/02/22, Modified: 2024/01/09

Plugin Output

tcp/0

## 101152 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3343-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3343-1 advisory.

- The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application.

(CVE-2014-9940)

- Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g.

Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line. (CVE-2017-1000363)

- The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device. (CVE-2017-7294)

- The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call. (CVE-2017-8890)

- The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls. (CVE-2017-9074)

- The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890. (CVE-2017-9075)

- The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890. (CVE-2017-9076)

- The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890. (CVE-2017-9077)

- The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls. (CVE-2017-9242)

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

## See Also

https://ubuntu.com/security/notices/USN-3343-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2014-9940 |
| CVE | CVE-2017-1000363 |
| CVE | CVE-2017-7294 |
| CVE | CVE-2017-8890 |
| CVE | CVE-2017-9074 |
| CVE | CVE-2017-9075 |
| CVE | CVE-2017-9076 |
| CVE | CVE-2017-9077 |
| CVE | CVE-2017-9242 |
| XREF | USN:3343-1 |

## Plugin Information

Published: 2017/06/30, Modified: 2024/01/09

Plugin Output

tcp/0

## 102261 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3381-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3381-1 advisory.

- An information disclosure vulnerability in kernel components including the ION subsystem, Binder, USB driver and networking subsystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31651010. (CVE-2016-8405)

- The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.

(CVE-2017-1000365)

- A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory. (CVE-2017-2618)

- In the Linux kernel before version 4.12, Kerberos 5 tickets decoded when using the RXRPC keys incorrectly assumes the size of a field. This could lead to the size-remaining variable wrapping and the data pointer going over the end of the buffer. This could possibly lead to memory corruption and possible privilege escalation. (CVE-2017-7482)

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

### See Also

https://ubuntu.com/security/notices/USN-3381-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-8405 |
| CVE | CVE-2017-1000365 |
| CVE | CVE-2017-2618 |
| CVE | CVE-2017-7482 |
| XREF | USN:3381-1 |

Plugin Information

Published: 2017/08/08, Modified: 2024/01/09

Plugin Output

tcp/0

## 102422 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3386-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3386-1 advisory.

- Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar:

lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW. (CVE-2017-1000111)

- Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ([IPv4/IPv6]: UFO Scatter-gather approach) on Oct 18 2005. (CVE-2017-1000112)

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

### See Also

https://ubuntu.com/security/notices/USN-3386-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

9.7

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-2017-1000111 |
| CVE | CVE-2017-1000112 |
| XREF | USN:3386-1 |

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/08/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 102820 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3406-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3406-1 advisory.

- The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.5.3 does not check whether a slot is a leaf, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (invalid pointer dereference and out-of-bounds read) via an application that uses associative-array data structures, as demonstrated by the keyutils test suite.

(CVE-2016-7914)

- The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.5 does not check for a zero value of certain levels data, which allows local users to cause a denial of service (ZERO_SIZE_PTR dereference, and GPF and possibly panic) via a crafted ioctl call for a /dev/dri/renderD* device. (CVE-2017-7261)

- The cp_report_fixup function in drivers/hid/hid-cypress.c in the Linux kernel 3.2 and 4.x before 4.9.4 allows physically proximate attackers to cause a denial of service (integer underflow) or possibly have unspecified other impact via a crafted HID report. (CVE-2017-7273)

- The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface. (CVE-2017-7487)

- fs/ext4/inode.c in the Linux kernel before 4.6.2, when ext4 data=ordered mode is used, mishandles a needs- flushing-before-commit list, which allows local users to obtain sensitive information from other users'

files in opportunistic circumstances by waiting for a hardware reset, creating a new file, making write system calls, and reading this file. (CVE-2017-7495)

- Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation. (CVE-2017-7616)

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

### See Also

https://ubuntu.com/security/notices/USN-3406-1

### Solution

Update the affected kernel package.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-7914 |
| CVE | CVE-2017-7261 |
| CVE | CVE-2017-7273 |
| CVE | CVE-2017-7487 |
| CVE | CVE-2017-7495 |
| CVE | CVE-2017-7616 |
| XREF | USN:3406-1 |

Plugin Information

Published: 2017/08/29, Modified: 2024/01/09

Plugin Output

tcp/0

## 103326 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3422-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3422-1 advisory.

- The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions, and consequently gain privileges, via an io_setup system call. (CVE-2016-10044)

- Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c. (CVE-2016-10200)

- The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. (CVE-2016-7097)

- The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent. (CVE-2016-8650)

- drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a state machine confusion bug. (CVE-2016-9083)

- drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file. (CVE-2016-9084)

- The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel before 4.7.5 does not initialize a certain integer variable, which allows local users to obtain sensitive information from kernel stack memory by triggering failure of a get_user_ex call. (CVE-2016-9178)

- The cgroup offline implementation in the Linux kernel through 4.8.11 mishandles certain drain operations, which allows local users to cause a denial of service (system hang) by leveraging access to a container environment for executing a crafted application, as demonstrated by trinity. (CVE-2016-9191)

- It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, such as '.dns_resolver' in RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass module signature verification by adding a new public key of its own devising to the keyring. (CVE-2016-9604)

- The ring_buffer_resize function in kernel/trace/ring_buffer.c in the profiling subsystem in the Linux kernel before 4.6.1 mishandles certain integer calculations, which allows local users to gain privileges by writing to the /sys/kernel/debug/tracing/buffer_size_kb file. (CVE-2016-9754)

- The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space. (CVE-2017-1000251)

- The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options. (CVE-2017-5970)

- The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag. (CVE-2017-6214)

- Race condition in net/packet/af_packet.c in the Linux kernel before 4.9.13 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a multithreaded application that makes PACKET_FANOUT setsockopt system calls. (CVE-2017-6346)

- The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a request_key system call for the dead type. (CVE-2017-6951)

- The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function. (CVE-2017-7187)

- The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.

(CVE-2017-7472)

- The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet. (CVE-2017-7541)

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

## See Also

https://ubuntu.com/security/notices/USN-3422-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-10044 |
| CVE | CVE-2016-10200 |
| CVE | CVE-2016-7097 |
| CVE | CVE-2016-8650 |
| CVE | CVE-2016-9083 |
| CVE | CVE-2016-9084 |
| CVE | CVE-2016-9178 |
| CVE | CVE-2016-9191 |
| CVE | CVE-2016-9604 |
| CVE | CVE-2016-9754 |
| CVE | CVE-2017-1000251 |
| CVE | CVE-2017-5970 |
| CVE | CVE-2017-6214 |
| CVE | CVE-2017-6346 |
| CVE | CVE-2017-6951 |
| CVE | CVE-2017-7187 |
| CVE | CVE-2017-7472 |
| CVE | CVE-2017-7541 |
| XREF | USN:3422-1 |

Plugin Information

Published: 2017/09/19, Modified: 2024/01/09

Plugin Output

tcp/0

## 104322 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3470-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3470-1 advisory.

- The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) by leveraging the CAP_NET_ADMIN capability. (CVE-2016-8632)

- Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing. (CVE-2017-10661)

- The sanity_check_raw_super function in fs/f2fs/super.c in the Linux kernel before 4.11.1 does not validate the segment count, which allows local users to gain privileges via unspecified vectors. (CVE-2017-10662)

- The sanity_check_ckpt function in fs/f2fs/super.c in the Linux kernel before 4.12.4 does not validate the blkoff and segno arrays, which allows local users to gain privileges via unspecified vectors.

(CVE-2017-10663)

- The make_response function in drivers/block/xen-blkback/blkback.c in the Linux kernel before 4.11.8 allows guest OS users to obtain sensitive information from host OS (or other guest OS) kernel memory by leveraging the copying of uninitialized padding fields in Xen block-interface response structures, aka XSA-216. (CVE-2017-10911)

- The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact. (CVE-2017-11176)

- The XFS_IS_REALTIME_INODE macro in fs/xfs/xfs_linux.h in the Linux kernel before 4.13.2 does not verify that a filesystem has a realtime device, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via vectors related to setting an RHINHERIT flag on a directory.

(CVE-2017-14340)

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

### See Also

https://ubuntu.com/security/notices/USN-3470-1

### Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.2

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-2016-8632 |
| CVE | CVE-2017-10661 |
| CVE | CVE-2017-10662 |
| CVE | CVE-2017-10663 |
| CVE | CVE-2017-10911 |
| CVE | CVE-2017-11176 |
| CVE | CVE-2017-14340 |
| XREF | USN:3470-1 |

Plugin Information

Published: 2017/11/01, Modified: 2024/01/09

Plugin Output

tcp/0

## 105106 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3510-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3510-1 advisory.

- The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd() function inside the THP implementation. touch_pmd() can be reached by get_user_pages(). In such case, the pmd will become dirty. This scenario breaks the new can_follow_write_pmd()'s logic - pmd can become dirty without going through a COW cycle. This bug is not as severe as the original Dirty cow because an ext4 file (or any other regular file) cannot be mapped using THP. Nevertheless, it does allow us to overwrite read-only huge pages. For example, the zero huge page and sealed shmem files can be overwritten (since their mapping can be populated using THP). Note that after the first write page-fault to the zero page, it will be replaced with a new fresh (and zeroed) thp. (CVE-2017-1000405)

- The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages. (CVE-2017-16939)

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

### See Also

https://ubuntu.com/security/notices/USN-3510-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

8.9

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-2017-1000405 |
| CVE | CVE-2017-16939 |
| XREF | USN:3510-1 |

Plugin Information

Published: 2017/12/08, Modified: 2024/01/09

Plugin Output

tcp/0

## 110050 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3655-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3655-1 advisory.

- The xen_biovec_phys_mergeable function in drivers/xen/biomerge.c in Xen might allow local OS guest users to corrupt block device data streams and consequently obtain sensitive memory information, cause a denial of service, or gain host OS privileges by leveraging incorrect block IO merge-ability calculation.

(CVE-2017-12134)

- An elevation of privilege vulnerability in the Upstream kernel bluez. Product: Android. Versions: Android kernel. Android ID: A-63527053. (CVE-2017-13220)

- A information disclosure vulnerability in the Upstream kernel encrypted-keys. Product: Android. Versions:

Android kernel. Android ID: A-70526974. (CVE-2017-13305)

- The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when CONFIG_NLMON is enabled, does not restrict observations of Netlink messages to a single net namespace, which allows local users to obtain sensitive information by leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system. (CVE-2017-17449)

- drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated. (CVE-2017-18079)

- The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices. (CVE-2017-18203)

- The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests. (CVE-2017-18204)

- The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.

(CVE-2017-18208)

- The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service (NR_MLOCK accounting corruption) via crafted use of mlockall and munlockall system calls. (CVE-2017-18221)

- Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4. (CVE-2018-3639)

- Incorrect buffer length handling in the ncp_read_kernel function in fs/ncpfs/ncplib_kernel.c in the Linux kernel through 4.15.11, and in drivers/staging/ncpfs/ncplib_kernel.c in the Linux kernel 4.16-rc through 4.16-rc6, could be exploited by malicious NCPFS servers to crash the kernel or execute code.

(CVE-2018-8822)

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

## See Also

https://ubuntu.com/security/notices/USN-3655-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2017-12134 |
| CVE | CVE-2017-13220 |
| CVE | CVE-2017-13305 |
| CVE | CVE-2017-17449 |
| CVE | CVE-2017-18079 |
| CVE | CVE-2017-18203 |
| CVE | CVE-2017-18204 |
| CVE | CVE-2017-18208 |
| CVE | CVE-2017-18221 |

| | |
|---|---|
| CVE | CVE-2018-3639 |
| CVE | CVE-2018-8822 |
| XREF | USN:3655-1 |

## Plugin Information

Published: 2018/05/23, Modified: 2024/01/09

## Plugin Output

tcp/0

## 110474 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3674-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3674-1 advisory.

- An information disclosure vulnerability in the kernel UVC driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18.

Android ID: A-33300353. (CVE-2017-0627)

- A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory. (CVE-2018-1068)

- A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related to RDS_GET_MR and RDS_GET_MR_FOR_DEST. (CVE-2018-7492)

- The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space. (CVE-2018-8781)

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

### See Also

https://ubuntu.com/security/notices/USN-3674-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-0627 |
| CVE | CVE-2018-1068 |
| CVE | CVE-2018-7492 |
| CVE | CVE-2018-8781 |
| XREF | USN:3674-1 |

Plugin Information

Published: 2018/06/12, Modified: 2024/01/09

Plugin Output

tcp/0

## 110900 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3698-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3698-1 advisory.

- The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the CR8-load exiting and CR8-store exiting L0 vmcs02 controls exist in cases where L1 omits the use TPR shadow vmcs12 control, which allows KVM L2 guest OS users to obtain read and write access to the hardware CR8 register. (CVE-2017-12154)

- The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations. (CVE-2017-12193)

- Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c. (CVE-2017-15265)

- Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls. (CVE-2018-1130)

- System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel. (CVE-2018-3665)

- The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading dmesg data from an SBS HC printk call.

(CVE-2018-5750)

- In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the

_sctp_make_chunk() function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash. (CVE-2018-5803)

- The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value. (CVE-2018-6927)

- An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR. (CVE-2018-7755)

- Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sas_phy directory, as demonstrated by the /sys/class/sas_phy/phy-1:0:12/ invalid_dword_count file. (CVE-2018-7757)

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

## See Also

https://ubuntu.com/security/notices/USN-3698-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2017-12154 |
| CVE | CVE-2017-12193 |
| CVE | CVE-2017-15265 |
| CVE | CVE-2018-1130 |
| CVE | CVE-2018-3665 |
| CVE | CVE-2018-5750 |
| CVE | CVE-2018-5803 |
| CVE | CVE-2018-6927 |
| CVE | CVE-2018-7755 |
| CVE | CVE-2018-7757 |
| XREF | USN:3698-1 |

## Plugin Information

Published: 2018/07/03, Modified: 2024/01/09

## Plugin Output

tcp/0

## 117869 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3775-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3775-1 advisory.

- A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a stack buffer overflow and smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Depending on how the target's code was built (i.e.

depending on a compiler, compile flags and hardware architecture) an attack may lead to a system crash and thus to a denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target.

Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x and 3.10.x are believed to be vulnerable. (CVE-2018-14633)

- An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.

(CVE-2018-14634)

- The spectre_v2_select_mitigation function in arch/x86/kernel/cpu/bugs.c in the Linux kernel before 4.18.1 does not always fill RSB upon a context switch, which makes it easier for attackers to conduct userspace-userspace spectreRSB attacks. (CVE-2018-15572)

- arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests. (CVE-2018-15594)

- Memory leak in the irda_bind function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket. (CVE-2018-6554)

- The irda_setsockopt function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket. (CVE-2018-6555)

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

### See Also

https://ubuntu.com/security/notices/USN-3775-1

### Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-14633 |
| CVE | CVE-2018-14634 |
| CVE | CVE-2018-15572 |
| CVE | CVE-2018-15594 |
| CVE | CVE-2018-6554 |
| CVE | CVE-2018-6555 |
| XREF | USN:3775-1 |

Plugin Information

Published: 2018/10/02, Modified: 2024/01/09

Plugin Output

tcp/0

## 118329 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3798-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3798-1 advisory.

- The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, security/keys/trusted.c, and security/keys/user_defined.c.

(CVE-2015-8539)

- The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure. (CVE-2016-7913)

- A elevation of privilege vulnerability in the Upstream kernel scsi driver. Product: Android. Versions:

Android kernel. Android ID: A-35644812. (CVE-2017-0794)

- The KEYS subsystem in the Linux kernel through 4.13.7 mishandles use of add_key for a key that already exists but is uninstantiated, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted system call.

(CVE-2017-15299)

- In fs/ocfs2/cluster/nodemanager.c in the Linux kernel before 4.15, local users can cause a denial of service (NULL pointer dereference and BUG) because a required mutex is not used. (CVE-2017-18216)

- In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition. (CVE-2018-1000004)

- The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user. (CVE-2018-7566)

- In nfc_llcp_build_sdreq_tlv of llcp_commands.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.

User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID:

A-73083945. (CVE-2018-9518)

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

### See Also

https://ubuntu.com/security/notices/USN-3798-1

### Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-8539 |
| CVE | CVE-2016-7913 |
| CVE | CVE-2017-0794 |
| CVE | CVE-2017-15299 |
| CVE | CVE-2017-18216 |
| CVE | CVE-2018-1000004 |
| CVE | CVE-2018-7566 |
| CVE | CVE-2018-9518 |
| XREF | USN:3798-1 |

Plugin Information

Published: 2018/10/23, Modified: 2024/01/09

Plugin Output

tcp/0

## 118973 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3822-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3822-1 advisory.

- arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest. (CVE-2016-9588)

- An elevation of privilege vulnerability in the kernel scsi driver. Product: Android. Versions: Android kernel. Android ID A-65023233. (CVE-2017-13168)

- The usbnet_generic_cdc_bind function in drivers/net/usb/cdc_ether.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device. (CVE-2017-16649)

- An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940. (CVE-2018-16658)

- In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds write with no additional execution privileges needed. User interaction is not needed for exploitation.

Product: Android Versions: Android kernel Android ID: A-65853588 References: Upstream kernel.

(CVE-2018-9363)

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

### See Also

https://ubuntu.com/security/notices/USN-3822-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-9588 |
| CVE | CVE-2017-13168 |
| CVE | CVE-2017-16649 |
| CVE | CVE-2018-16658 |
| CVE | CVE-2018-9363 |
| XREF | USN:3822-1 |

Plugin Information

Published: 2018/11/15, Modified: 2024/01/09

Plugin Output

tcp/0

## 119832 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3849-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3849-1 advisory.

- The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for a certain match field, related to the keyring_search_iterator function in keyring.c. (CVE-2017-2647)

- It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation. (CVE-2018-10902)

- An issue was discovered in the Linux kernel through 4.17.3. An Integer Overflow in kernel/time/posix-timers.c in the POSIX timer code is caused by the way the overrun accounting works. Depending on interval and expiry time values, the overrun can be larger than INT_MAX, but the accounting is int based. This basically makes the accounting values, which are visible to user space via timer_getoverrun(2) and siginfo::si_overrun, random. For example, a local user can cause a denial of service (signed integer overflow) via crafted mmap, futex, timer_create, and timer_settime system calls. (CVE-2018-12896)

- drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free). (CVE-2018-14734)

- An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges. (CVE-2018-16276)

- drivers/tty/n_tty.c in the Linux kernel before 4.14.11 allows local attackers (who are able to access pseudo terminals) to hang/block further usage of any pseudo terminal devices due to an EXTPROC versus ICANON confusion in TIOCINQ. (CVE-2018-18386)

- In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form. (CVE-2018-18690)

- An issue was discovered in the Linux kernel through 4.19. An information leak in cdrom_ioctl_select_disc in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940 and CVE-2018-16658. (CVE-2018-18710)

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

### See Also

https://ubuntu.com/security/notices/USN-3849-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2017-2647 |
| CVE | CVE-2018-10902 |
| CVE | CVE-2018-12896 |
| CVE | CVE-2018-14734 |
| CVE | CVE-2018-16276 |
| CVE | CVE-2018-18386 |
| CVE | CVE-2018-18690 |
| CVE | CVE-2018-18710 |
| XREF | USN:3849-1 |

## Plugin Information

Published: 2018/12/21, Modified: 2024/01/09

## Plugin Output

tcp/0

## 121598 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3880-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3880-1 advisory.

- The Linux kernel before version 4.11 is vulnerable to a NULL pointer dereference in fs/cifs/cifsencrypt.c:setup_ntlmv2_rsp() that allows an attacker controlling a CIFS server to kernel panic a client that has this server mounted, because an empty TargetInfo field in an NTLMSSP setup negotiation response is mishandled during session recovery. (CVE-2018-1066)

- An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents. (CVE-2018-17972)

- Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks.

If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remain for a short time that permits access to a physical page after it has been released back to the page allocator and reused. This is fixed in the following kernel versions:

4.9.135, 4.14.78, 4.18.16, 4.19. (CVE-2018-18281)

- In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References:

Upstream kernel. (CVE-2018-9568)

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

### See Also

https://ubuntu.com/security/notices/USN-3880-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-1066 |
| CVE | CVE-2018-17972 |
| CVE | CVE-2018-18281 |
| CVE | CVE-2018-9568 |
| XREF | USN:3880-1 |

Plugin Information

Published: 2019/02/05, Modified: 2024/01/09

Plugin Output

tcp/0

## 123682 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3933-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3933-1 advisory.

- The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void

*)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes). (CVE-2017-1000410)

- In change_port_settings in drivers/usb/serial/io_ti.c in the Linux kernel before 4.11.3, local users could cause a denial of service by division-by-zero in the serial device layer by trying to set very high baud rates. (CVE-2017-18360)

- In the Linux kernel through 4.19.6, a local user could exploit a use-after-free in the ALSA driver by supplying a malicious USB Sound device (with zero interfaces) that is mishandled in usb_audio_probe in sound/usb/card.c. (CVE-2018-19824)

- A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. (CVE-2019-3459)

- A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1. (CVE-2019-3460)

- In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free. (CVE-2019-6974)

- The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak. (CVE-2019-7222)

- In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task. (CVE-2019-9213)

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

## See Also

https://ubuntu.com/security/notices/USN-3933-1

## Solution

Update the affected kernel 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

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

## VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2017-1000410 |
| CVE | CVE-2017-18360 |
| CVE | CVE-2018-19824 |
| CVE | CVE-2019-3459 |
| CVE | CVE-2019-3460 |
| CVE | CVE-2019-6974 |
| CVE | CVE-2019-7222 |
| CVE | CVE-2019-9213 |
| XREF | USN:3933-1 |

## Exploitable With

Metasploit (true)

## Plugin Information

Published: 2019/04/03, Modified: 2024/01/09

## Plugin Output

tcp/0

## 192221 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-6699-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6699-1 advisory.

- An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4. (CVE-2023-30456)

- A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d8. (CVE-2023-4921)

- A race condition was found in the Linux kernel's scsi device driver in lpfc_unregister_fcf_rescan() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue. (CVE-2024-24855)

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

### See Also

https://ubuntu.com/security/notices/USN-6699-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-4921 |
| CVE | CVE-2023-30456 |
| CVE | CVE-2024-24855 |
| XREF | USN:6699-1 |

## Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

## Plugin Output

tcp/0

## 76386 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2274-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2274-1 advisory.

- The Linux kernel before 3.15.4 on Intel processors does not properly restrict use of a non-canonical value for the saved RIP address in the case of a system call that does not use IRET, which allows local users to leverage a race condition and gain privileges, or cause a denial of service (double fault), via a crafted application that makes ptrace and fork system calls. (CVE-2014-4699)

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

### See Also

https://ubuntu.com/security/notices/USN-2274-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

8.4

### 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:2274-1 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2014/07/06, Modified: 2024/01/09

## Plugin Output

tcp/0

## 77199 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2314-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2314-1 advisory.

- kernel/auditsc.c in the Linux kernel through 3.14.5, when CONFIG_AUDITSYSCALL is enabled with certain syscall rules, allows local users to obtain potentially sensitive single-bit values from kernel memory or cause a denial of service (OOPS) via a large value of a syscall number. (CVE-2014-3917)

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

### See Also

https://ubuntu.com/security/notices/USN-2314-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.2

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| BID | 67699 |
| CVE | CVE-2014-3917 |
| XREF | USN:2314-1 |

## Plugin Information

Published: 2014/08/14, Modified: 2024/01/09

## Plugin Output

tcp/0

## 81774 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2528-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2528-1 advisory.

- The InfiniBand (IB) implementation in the Linux kernel package before 2.6.32-504.12.2 on Red Hat Enterprise Linux (RHEL) 6 does not properly restrict use of User Verbs for registration of memory regions, which allows local users to access arbitrary physical memory locations, and consequently cause a denial of service (system crash) or gain privileges, by leveraging permissions on a uverbs device under /dev/infiniband/. (CVE-2014-8159)

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

### See Also

https://ubuntu.com/security/notices/USN-2528-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 73060 |
| CVE | CVE-2014-8159 |
| XREF | USN:2528-1 |

Plugin Information

Published: 2015/03/12, Modified: 2024/01/09

Plugin Output

tcp/0

## 83259 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2598-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2598-1 advisory.

- Race condition in the prepare_binprm function in fs/exec.c in the Linux kernel before 3.19.6 allows local users to gain privileges by executing a setuid program at a time instant when a chown to root is in progress, and the ownership is changed but the setuid bit is not yet stripped. (CVE-2015-3339)

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

### See Also

https://ubuntu.com/security/notices/USN-2598-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-3339 |
| XREF | USN:2598-1 |

Plugin Information

Published: 2015/05/06, Modified: 2024/01/09

Plugin Output

tcp/0

## 83811 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2620-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2620-1 advisory.

- A certain backport in the TCP Fast Open implementation for the Linux kernel before 3.18 does not properly maintain a count value, which allow local users to cause a denial of service (system crash) via the Fast Open feature, as demonstrated by visiting the chrome://flags/#enable-tcp-fast-open URL when using certain 3.10.x through 3.16.x kernel builds, including longterm-maintenance releases and ckt (aka Canonical Kernel Team) builds. (CVE-2015-3332)

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

### See Also

https://ubuntu.com/security/notices/USN-2620-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 74232 |
| CVE | CVE-2015-3332 |
| XREF | USN:2620-1 |

Plugin Information

Published: 2015/05/26, Modified: 2024/01/09

Plugin Output

tcp/0

## 84210 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2643-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2643-1 advisory.

- The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a configuration in which overlayfs is permitted in an arbitrary mount namespace. (CVE-2015-1328)

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

### See Also

https://ubuntu.com/security/notices/USN-2643-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.7

### 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-2015-1328 |
| XREF | USN:2643-1 |

Exploitable With

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

Plugin Information

Published: 2015/06/16, Modified: 2024/01/09

Plugin Output

tcp/0

## 86295 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2761-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2761-1 advisory.

- Race condition in the IPC object implementation in the Linux kernel through 4.2.3 allows local users to gain privileges by triggering an ipc_addid call that leads to uid and gid comparisons against uninitialized data, related to msg.c, shm.c, and util.c. (CVE-2015-7613)

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

### See Also

https://ubuntu.com/security/notices/USN-2761-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-7613 |
| XREF | USN:2761-1 |

Plugin Information

Published: 2015/10/06, Modified: 2024/01/09

Plugin Output

tcp/0

## 88010 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2870-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2870-1 advisory.

- The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands. (CVE-2016-0728)

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

### See Also

https://ubuntu.com/security/notices/USN-2870-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.6

### 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-2016-0728 |
| XREF | USN:2870-1 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2016/01/20, Modified: 2024/01/09

Plugin Output

tcp/0

## 91181 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2975-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2975-1 advisory.

- Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data. (CVE-2016-0758)

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

### See Also

https://ubuntu.com/security/notices/USN-2975-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-0758 |
| XREF | USN:2975-1 |

Plugin Information

Published: 2016/05/17, Modified: 2024/01/09

Plugin Output

tcp/0

## 91561 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2999-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2999-1 advisory.

- The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mmap calls for /proc pathnames, leading to recursive pagefault handling. (CVE-2016-1583)

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

### See Also

https://ubuntu.com/security/notices/USN-2999-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-1583 |
| XREF | USN:2999-1 |

Plugin Information

Published: 2016/06/10, Modified: 2024/01/09

Plugin Output

tcp/0

## 92313 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3034-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3034-1 advisory.

- The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by triggering a certain page move. (CVE-2016-3070)

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

### See Also

https://ubuntu.com/security/notices/USN-3034-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-3070 |
| XREF | USN:3034-1 |

Plugin Information

Published: 2016/07/15, Modified: 2024/01/09

Plugin Output

tcp/0

## 94153 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3105-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3105-1 advisory.

- Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka Dirty COW. (CVE-2016-5195)

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

### See Also

https://ubuntu.com/security/notices/USN-3105-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.8

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2016-5195 |
| XREF | USN:3105-1 |
| XREF | IAVA:2016-A-0306-S |
| XREF | CISA-KNOWN-EXPLOITED:2022/03/24 |

## Exploitable With

CANVAS (true) Core Impact (true)

## Plugin Information

Published: 2016/10/20, Modified: 2024/01/09

## Plugin Output

tcp/0

## 95566 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3149-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3149-1 advisory.

- Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions. (CVE-2016-8655)

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

### See Also

https://ubuntu.com/security/notices/USN-3149-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.6

### 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-2016-8655 |
| XREF | USN:3149-1 |

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2016/12/06, Modified: 2024/01/09

Plugin Output

tcp/0

## 97603 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3219-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3219-1 advisory.

- Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline. (CVE-2017-2636)

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

### See Also

https://ubuntu.com/security/notices/USN-3219-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-2636 |
| XREF | USN:3219-1 |

Plugin Information

Published: 2017/03/08, Modified: 2024/01/09

Plugin Output

tcp/0

## 99098 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3250-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3250-1 advisory.

- The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux- image-* package 4.8.0.41.52. (CVE-2017-7184)

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

### See Also

https://ubuntu.com/security/notices/USN-3250-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-7184 |
| XREF | USN:3250-1 |

Plugin Information

Published: 2017/03/30, Modified: 2024/01/09

Plugin Output

tcp/0

## 100933 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3335-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3335-1 advisory.

- An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be jumped over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010). (CVE-2017-1000364)

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

### See Also

https://ubuntu.com/security/notices/USN-3335-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-1000364 |
| XREF | USN:3335-1 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2017/06/20, Modified: 2024/01/09

Plugin Output

tcp/0

## 125135 - Ubuntu 14.04 LTS : samba vulnerability (USN-3976-2)

### Synopsis

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

### Description

USN-3976-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.

Original advisory details :

Isaac Boukris and Andrew Bartlett discovered that Samba incorrectly checked S4U2Self packets. In certain environments, a remote attacker could possibly use this issue to escalate 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/3976-2/

### Solution

Update the affected samba package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-16860 |
| XREF | USN:3976-2 |

Plugin Information

Published: 2019/05/15, Modified: 2024/05/22

Plugin Output

tcp/0

## 125475 - Ubuntu 14.04 LTS : samba vulnerability (USN-3976-4)

### Synopsis

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

### Description

USN-3976-1 fixed a vulnerability in Samba. The update introduced a regression causing Samba to occasionally crash. This update fixes the problem.

Original advisory details :

Isaac Boukris and Andrew Bartlett discovered that Samba incorrectly checked S4U2Self packets. In certain environments, a remote attacker could possibly use this issue to escalate 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/3976-4/

### Solution

Update the affected samba package.

### Risk Factor

High

### References

| | |
|---|---|
| XREF | USN:3976-4 |

### Plugin Information

Published: 2019/05/28, Modified: 2023/01/17

### Plugin Output

tcp/0

## 40984 - Browsable Web Directories

### Synopsis

Some directories on the remote web server are browsable.

### Description

Multiple Nessus plugins identified directories on the web server that are browsable.

### See Also

http://www.nessus.org/u?0a35179e

### Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

### 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: 2009/09/15, Modified: 2021/01/19

### Plugin Output

tcp/80/www

## 47831 - CGI Generic XSS (comprehensive test)

### Synopsis

The remote web server is prone to cross-site scripting attacks.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected'.

### See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

### Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:80 |
| XREF | CWE:81 |
| XREF | CWE:83 |
| XREF | CWE:84 |
| XREF | CWE:85 |
| XREF | CWE:86 |
| XREF | CWE:87 |
| XREF | CWE:116 |
| XREF | CWE:442 |
| XREF | CWE:692 |

| | |
|---|---|
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:751 |
| XREF | CWE:801 |
| XREF | CWE:811 |
| XREF | CWE:928 |
| XREF | CWE:931 |

## Plugin Information

Published: 2010/07/26, Modified: 2022/04/11

## Plugin Output

tcp/80/www

```
Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (comprehensive test) :

+ The 'user' parameter of the /payroll_app.php CGI :

/payroll_app.php [password=&s=OK&user=<%00script>alert(219);</script%00>
]
```

## 50686 - IP Forwarding Enabled

### Synopsis

The remote host has IP forwarding enabled.

### Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

### Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### VPR Score

4.0

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| CVE | CVE-1999-0511 |

### Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

## 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

### 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

## 192685 - Node.js Module node-tar < 6.2.1 DoS

### Synopsis

A module in the Node.js JavaScript run-time environment is affected by a denial of service vulnerability.

### Description

In the nodejs module node-tar prior to version 6.2.1, there is no validation of the number of folders created while unpacking a file. As a result, an attacker can use a malicious file to exhaust the CPU and memory on the host and crash the nodejs client.

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?0b8d8923

### Solution

Upgrade to node-tar version 6.2.1 or later.

### 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

4.4

### 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)

### STIG Severity

II

References

| | |
|---|---|
| CVE | CVE-2024-28863 |
| XREF | IAVB:2024-B-0027 |

Plugin Information

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

Plugin Output

tcp/0

## 64993 - PHP 5.4.x < 5.4.12 Information Disclosure

### Synopsis

The remote web server uses a version of PHP that is potentially affected by an information disclosure vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.12. It is, therefore, potentially affected by an information disclosure in the file 'ext/soap/php_xml.c'

related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1824)

Note that this plugin does not attempt to exploit the vulnerabilities but, instead relies only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.12

http://www.nessus.org/u?2dcf53bd

http://www.nessus.org/u?889595b1

### Solution

Upgrade to PHP version 5.4.12 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

1.4

### 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 | 62373 |
| CVE | CVE-2013-1824 |

Plugin Information

Published: 2013/03/04, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 66843 - PHP 5.4.x < 5.4.16 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.16. It is, therefore, potentially affected by the following vulnerabilities:

- An error exists in the mimetype detection of 'mp3' files that could lead to a denial of service. (Bug #64830)

- An error exists in the function 'php_quot_print_encode'

in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings. (Bug #64879)

- An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c'

that could allow denial of service attacks. (Bug #64895)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

### See Also

http://www.nessus.org/u?60cbc5f0

http://www.nessus.org/u?8456482e

http://www.php.net/ChangeLog-5.php#5.4.16

### Solution

Apply the vendor patch or upgrade to PHP version 5.4.16 or later.

### Risk Factor

Medium

### VPR Score

3.6

### 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 | 60411 |
| BID | 60728 |
| BID | 60731 |
| CVE | CVE-2013-2110 |
| CVE | CVE-2013-4635 |
| CVE | CVE-2013-4636 |

## Plugin Information

Published: 2013/06/07, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 71927 - PHP 5.4.x < 5.4.24 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.24. It is, therefore, potentially affected by the following vulnerabilities :

- A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that could allow denial of service attacks. (CVE-2013-6712)

- An integer overflow error exists in the function 'exif_process_IFD_TAG' in the file 'ext/exif/exif.c'

that could allow denial of service attacks or arbitrary memory reads. (Bug #65873)

Note that this plugin does not attempt to exploit the vulnerabilities, but instead relies only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.24

### Solution

Upgrade to PHP version 5.4.24 or later.

### Risk Factor

Medium

### VPR Score

4.4

### 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 | 64018 |
| CVE | CVE-2013-6712 |

## Plugin Information

Published: 2014/01/13, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 72881 - PHP 5.4.x < 5.4.26 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.26. It is, therefore, potentially affected by the following vulnerabilities :

- An error exists related to the Fileinfo extension and the bundled libmagic library that could allow denial of service attacks. (CVE-2014-1943)

- An error exists related to the Fileinfo extension and the process of analyzing Portable Executable (PE) format files that could allow denial of service attacks or possibly arbitrary code execution. (CVE-2014-2270)

Note that this plugin does not attempt to exploit the vulnerabilities, but instead relies only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.26

### Solution

Upgrade to PHP version 5.4.26 or later.

### Risk Factor

Medium

### VPR Score

3.6

### 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 | 65596 |
| BID | 66002 |
| CVE | CVE-2014-1943 |

CVE CVE-2014-2270

## Plugin Information

Published: 2014/03/07, Modified: 2024/05/31

## Plugin Output

tcp/80/www

## 73338 - PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS

### Synopsis

The remote web server uses a version of PHP that is potentially affected by a denial of service vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.27. It is, therefore, potentially affected by a denial of service vulnerability.

A flaw exists in the awk script detector within magic/Magdir/commands where multiple wildcards with unlimited repetitions are used. This could allow a context dependent attacker to cause a denial of service with a specially crafted ASCII file.

Note that this plugin has not attempted to exploit this issue, but instead relied only on PHP's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.27

### Solution

Upgrade to PHP version 5.4.27 or later.

### Risk Factor

Medium

### VPR Score

4.2

### 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 | 66406 |
| CVE | CVE-2013-7345 |

### Plugin Information

Published: 2014/04/04, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 74291 - PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.29. It is, therefore, affected by the following vulnerabilities :

- A flaw exists with the 'cdf_unpack_summary_info()'

function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.

This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

- A flaw exists with the 'cdf_read_property_info()'

function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

- An out-of-bounds read exists in printf. (Bug #67249)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.29

https://bugs.php.net/bug.php?id=67327

https://bugs.php.net/bug.php?id=67328

### Solution

Upgrade to PHP version 5.4.29 or later.

### Risk Factor

Medium

### VPR Score

3.6

### 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 | 67759 |
| BID | 67765 |
| BID | 69271 |
| CVE | CVE-2014-0237 |
| CVE | CVE-2014-0238 |

Plugin Information

Published: 2014/06/03, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 77402 - PHP 5.4.x < 5.4.32 Multiple Vulnerabilities

### Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

### Description

According to its banner, the remote web server is running a version of PHP 5.4.x prior to 5.4.32. It is, therefore, affected by the following vulnerabilities :

- LibGD contains a NULL pointer dereference flaw in its 'gdImageCreateFromXpm' function in the 'gdxpm.c' file.

By using a specially crafted color mapping, a remote attacker could cause a denial of service.

(CVE-2014-2497)

- The original upstream patch for CVE-2013-7345 did not provide a complete solution. It is, therefore, still possible for a remote attacker to deploy a specially crafted input file to cause excessive resources to be used when trying to detect the file type using awk regular expression rules. This can cause a denial of service. (CVE-2014-3538)

- An integer overflow flaw exists in the 'cdf.c' file. By using a specially crafted CDF file, a remote attacker could cause a denial of service. (CVE-2014-3587)

- There are multiple buffer overflow flaws in the 'dns.c'

file related to the 'dns_get_record' and 'dn_expand'

functions. By using a specially crafted DNS record, a remote attacker could exploit these to cause a denial of service or execute arbitrary code. (CVE-2014-3597)

- A flaw exists in the 'spl_dllist.c' file that may lead to a use-after-free condition in the SPL component when iterating over an object. An attacker could utilize this to cause a denial of service. (CVE-2014-4670)

- A flaw exists in the 'spl_array.c' file that may lead to a use-after-free condition in the SPL component when handling the modification of objects while sorting. An attacker could utilize this to cause a denial of service. (CVE-2014-4698)

- There exist multiple flaws in the GD component within the 'gd_ctx.c' file where user-supplied input is not properly validated to ensure that pathnames lack %00 sequences. By using specially crafted input, a remote attacker could overwrite arbitrary files.

(CVE-2014-5120)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.32

https://bugs.php.net/bug.php?id=67730

https://bugs.php.net/bug.php?id=67538

https://bugs.php.net/bug.php?id=67539

https://bugs.php.net/bug.php?id=67717

https://bugs.php.net/bug.php?id=67705
https://bugs.php.net/bug.php?id=67716
https://bugs.php.net/bug.php?id=66901
https://bugs.php.net/bug.php?id=67715

## Solution

Upgrade to PHP version 5.4.32 or later.

## Risk Factor

Medium

## VPR Score

5.9

## 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

| | |
|---|---|
| BID | 66233 |
| BID | 66406 |
| BID | 68348 |
| BID | 68511 |
| BID | 68513 |
| BID | 69322 |
| BID | 69325 |
| BID | 69375 |
| CVE | CVE-2014-2497 |
| CVE | CVE-2014-3538 |
| CVE | CVE-2014-3587 |
| CVE | CVE-2014-3597 |
| CVE | CVE-2014-4670 |
| CVE | CVE-2014-4698 |
| CVE | CVE-2014-5120 |

## Plugin Information

Published: 2014/08/27, Modified: 2024/05/28

Plugin Output

tcp/80/www

## 79246 - PHP 5.4.x < 5.4.35 'donote' DoS

### Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is prior to 5.4.35. It is, therefore, affected by an out-of-bounds read error in the function 'donote' within the file 'ext/fileinfo/libmagic/readelf.c' that could allow application crashes.

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

### See Also

http://php.net/ChangeLog-5.php#5.4.35

https://bugs.php.net/bug.php?id=68283

http://www.nessus.org/u?6f0615b4

### Solution

Upgrade to PHP version 5.4.35 or later.

### Risk Factor

Medium

### VPR Score

3.6

### 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 | 70807 |
| CVE | CVE-2014-3710 |

### Plugin Information

Published: 2014/11/14, Modified: 2024/05/31

Plugin Output

tcp/80/www

## 152853 - PHP < 7.3.28 Email Header Injection

### Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

### Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28.

It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

### See Also

https://www.php.net/ChangeLog-7.php#7.3.28

### Solution

Upgrade to PHP version 7.3.28 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2021/08/26, Modified: 2024/06/04

### Plugin Output

tcp/80/www

## 46803 - PHP expose_php Information Disclosure

### Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

### Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

### See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

### Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2010/06/03, Modified: 2022/04/11

### Plugin Output

tcp/80/www

## 57608 - SMB Signing not required

### Synopsis

Signing is not required on the remote SMB server.

### Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

### See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

### Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

## 187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

### Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

### Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

### See Also

https://terrapin-attack.com/

### Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.1

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-48795 |

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

## 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

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

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

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

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

### See Also

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

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

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

tcp/631/www

## 45411 - SSL Certificate with Wrong Hostname

### Synopsis

The SSL certificate for this service is for a different host.

### Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

### Plugin Output

tcp/631/www

```
The identities known by Nessus are :

  10.0.2.9
  127.0.0.1
  172.17.0.1
  ::1
  ['ipv6': ::1]['scope': host]['prefixlen': 128]
  ['ipv6': fe80::42:5dff:feb4:5086]['scope': link]['prefixlen': 64]
  ['ipv6': fe80::6417:fcff:fe53:af9b]['scope': link]['prefixlen': 64]
  ['ipv6': fe80::a00:27ff:fe0e:2bcc]['scope': link]['prefixlen': 64]
  fe80::42:5dff:feb4:5086
  fe80::6417:fcff:fe53:af9b
  fe80::a00:27ff:fe0e:2bcc
  metasploitable3-ub1404
  10.0.2.9

The Common Name in the certificate is :
```

```
    ubuntu
```

## 57582 - SSL Self-Signed Certificate

### Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

### Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

### Plugin Output

tcp/631/www

## 58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

### Synopsis

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.

If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL \SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

### See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.imperialviolet.org/2011/09/23/chromeandbeast.html

https://vnhacker.blogspot.com/2011/09/beast.html

http://www.nessus.org/u?649b81c1

http://www.nessus.org/u?84775fd6

https://blogs.msdn.microsoft.com/kaushal/2012/01/20/fixing-the-beast/

### Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.

Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

2.9

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)

STIG Severity

I

References

| | |
|---|---|
| BID | 49778 |
| CVE | CVE-2011-3389 |
| XREF | CERT:864643 |
| XREF | MSFT:MS12-006 |
| XREF | IAVB:2012-B-0006 |
| XREF | CEA-ID:CEA-2019-0547 |

Plugin Information

Published: 2012/04/16, Modified: 2022/12/05

Plugin Output

tcp/631/www

## 104743 - TLS Version 1.0 Protocol Detection

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

### See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

### Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### References

XREF CWE:327

### Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

### Plugin Output

tcp/631/www

## 157288 - TLS Version 1.1 Deprecated Protocol

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

### See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

### Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:327 |

### Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

### Plugin Output

tcp/631/www

## 200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a

denial of service, or possibly execute arbitrary code.

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

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

### See Also

https://ubuntu.com/security/notices/USN-6827-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-3164 |
| XREF | USN:6827-1 |

Plugin Information

Published: 2024/06/11, Modified: 2024/06/11

Plugin Output

tcp/0

## 190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

- A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.

(CVE-2023-4641)

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

### See Also

https://ubuntu.com/security/notices/USN-6640-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-4641 |
| XREF | USN:6640-1 |

Plugin Information

Published: 2024/02/15, Modified: 2024/02/15

Plugin Output

tcp/0

## 192577 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6588-2 advisory.

- linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY. (CVE-2024-22365)

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

### See Also

https://ubuntu.com/security/notices/USN-6588-2

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-22365 |
| XREF | USN:6588-2 |

Plugin Information

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

Plugin Output

tcp/0

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

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

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

- NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().

(CVE-2023-50495)

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

### See Also

https://ubuntu.com/security/notices/USN-6684-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/0

## 83332 - Ubuntu 14.04 LTS : Linux kernel regression (USN-2598-2)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2598-2 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-2598-2

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### References

| | |
|---|---|
| BID | 74243 |
| XREF | USN:2598-2 |

### Plugin Information

Published: 2015/05/11, Modified: 2024/01/09

### Plugin Output

tcp/0

## 112017 - Ubuntu 14.04 LTS : Linux kernel regressions (USN-3741-3)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3741-3 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-3741-3

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### VPR Score

5.2

### References

| | |
|---|---|
| CVE | CVE-2018-3620 |
| CVE | CVE-2018-3646 |
| CVE | CVE-2018-5390 |
| CVE | CVE-2018-5391 |
| XREF | USN:3741-3 |

### Plugin Information

Published: 2018/08/20, Modified: 2024/01/09

### Plugin Output

tcp/0

## 74360 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2240-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2240-1 advisory.

- Use-after-free vulnerability in the nfqnl_zcopy function in net/netfilter/nfnetlink_queue_core.c in the Linux kernel through 3.13.6 allows attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphaning operation. NOTE: the affected code was moved to the skb_zerocopy function in net/core/skbuff.c before the vulnerability was announced. (CVE-2014-2568)

- The try_to_unmap_cluster function in mm/rmap.c in the Linux kernel before 3.14.3 does not properly consider which pages must be locked, which allows local users to cause a denial of service (system crash) by triggering a memory-usage pattern that requires removal of page-table mappings. (CVE-2014-3122)

- The futex_requeue function in kernel/futex.c in the Linux kernel through 3.14.5 does not ensure that calls have two different futex addresses, which allows local users to gain privileges via a crafted FUTEX_REQUEUE command that facilitates unsafe waiter modification. (CVE-2014-3153)

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

### See Also

https://ubuntu.com/security/notices/USN-2240-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

9.7

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

| | |
|---|---|
| BID | 66348 |
| CVE | CVE-2014-2568 |
| CVE | CVE-2014-3122 |
| CVE | CVE-2014-3153 |
| XREF | USN:2240-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/06/15 |

Exploitable With

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

Plugin Information

Published: 2014/06/06, Modified: 2024/01/09

Plugin Output

tcp/0

## 76569 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2290-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2290-1 advisory.

- The media_device_enum_entities function in drivers/media/media-device.c in the Linux kernel before 3.14.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging /dev/media0 read access for a MEDIA_IOC_ENUM_ENTITIES ioctl call.

(CVE-2014-1739)

- The (1) BPF_S_ANC_NLATTR and (2) BPF_S_ANC_NLATTR_NEST extension implementations in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 do not check whether a certain length value is sufficiently large, which allows local users to cause a denial of service (integer underflow and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr and

__skb_get_nlattr_nest functions before the vulnerability was announced. (CVE-2014-3144)

- The BPF_S_ANC_NLATTR_NEST extension implementation in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 uses the reverse order in a certain subtraction, which allows local users to cause a denial of service (over-read and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr_nest function before the vulnerability was announced.

(CVE-2014-3145)

- The Linux kernel through 3.14.5 does not properly consider the presence of hugetlb entries, which allows local users to cause a denial of service (memory corruption or system crash) by accessing certain memory locations, as demonstrated by triggering a race condition via numa_maps read operations during hugepage migration, related to fs/proc/task_mmu.c and mm/mempolicy.c. (CVE-2014-3940)

- Integer overflow in the LZ4 algorithm implementation, as used in Yann Collet LZ4 before r118 and in the lz4_uncompress function in lib/lz4/lz4_decompress.c in the Linux kernel before 3.15.2, on 32-bit platforms might allow context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted Literal Run that would be improperly handled by programs not complying with an API limitation, a different vulnerability than CVE-2014-4715. (CVE-2014-4611)

- The PPPoL2TP feature in net/l2tp/l2tp_ppp.c in the Linux kernel through 3.15.6 allows local users to gain privileges by leveraging data-structure differences between an l2tp socket and an inet socket.

(CVE-2014-4943)

- The net_get_random_once implementation in net/core/utils.c in the Linux kernel 3.13.x and 3.14.x before 3.14.5 on certain Intel processors does not perform the intended slow-path operation to initialize random seeds, which makes it easier for remote attackers to spoof or disrupt IP communication by leveraging the predictability of TCP sequence numbers, TCP and UDP port numbers, and IP ID values. (CVE-2014-7284)

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

### See Also

https://ubuntu.com/security/notices/USN-2290-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

8.9

## 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 | 67309 |
| BID | 67321 |
| BID | 67786 |
| BID | 68048 |
| BID | 68214 |
| BID | 68218 |
| BID | 68683 |
| CVE | CVE-2014-1739 |
| CVE | CVE-2014-3144 |
| CVE | CVE-2014-3145 |
| CVE | CVE-2014-3940 |
| CVE | CVE-2014-4611 |
| CVE | CVE-2014-4943 |
| CVE | CVE-2014-7284 |
| XREF | USN:2290-1 |

## Exploitable With

CANVAS (true)

## Plugin Information

Published: 2014/07/17, Modified: 2024/01/09

## Plugin Output

tcp/0

## 78765 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2395-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2395-1 advisory.

- Array index error in the logi_dj_raw_event function in drivers/hid/hid-logitech-dj.c in the Linux kernel before 3.16.2 allows physically proximate attackers to execute arbitrary code or cause a denial of service (invalid kfree) via a crafted device that provides a malformed REPORT_TYPE_NOTIF_DEVICE_UNPAIRED value.

(CVE-2014-3182)

- The WRMSR processing functionality in the KVM subsystem in the Linux kernel through 3.17.2 does not properly handle the writing of a non-canonical address to a model-specific register, which allows guest OS users to cause a denial of service (host OS crash) by leveraging guest OS privileges, related to the wrmsr_interception function in arch/x86/kvm/svm.c and the handle_wrmsr function in arch/x86/kvm/vmx.c.

(CVE-2014-3610)

- Race condition in the __kvm_migrate_pit_timer function in arch/x86/kvm/i8254.c in the KVM subsystem in the Linux kernel through 3.17.2 allows guest OS users to cause a denial of service (host OS crash) by leveraging incorrect PIT emulation. (CVE-2014-3611)

- arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel through 3.17.2 does not have an exit handler for the INVVPID instruction, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application. (CVE-2014-3646)

- arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel through 3.17.2 does not properly perform RIP changes, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application. (CVE-2014-3647)

- The SMB2_tcon function in fs/cifs/smb2pdu.c in the Linux kernel before 3.16.3 allows remote CIFS servers to cause a denial of service (NULL pointer dereference and client system crash) or possibly have unspecified other impact by deleting the IPC$ share during resolution of DFS referrals. (CVE-2014-7145)

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

### See Also

https://ubuntu.com/security/notices/USN-2395-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 69867 |
| BID | 70742 |
| BID | 70743 |
| BID | 70745 |
| BID | 70748 |
| CVE | CVE-2014-3182 |
| CVE | CVE-2014-3610 |
| CVE | CVE-2014-3611 |
| CVE | CVE-2014-3646 |
| CVE | CVE-2014-3647 |
| CVE | CVE-2014-7145 |
| XREF | USN:2395-1 |

Plugin Information

Published: 2014/10/31, Modified: 2024/01/09

Plugin Output

tcp/0

## 79435 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2420-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2420-1 advisory.

- arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel before 3.17.2 on Intel processors does not ensure that the value in the CR4 control register remains the same after a VM entry, which allows host OS users to kill arbitrary processes or cause a denial of service (system disruption) by leveraging /dev/kvm access, as demonstrated by PR_SET_TSC prctl calls within a modified copy of QEMU. (CVE-2014-3690)

- Multiple integer overflows in the lzo1x_decompress_safe function in lib/lzo/lzo1x_decompress_safe.c in the LZO decompressor in the Linux kernel before 3.15.2 allow context-dependent attackers to cause a denial of service (memory corruption) via a crafted Literal Run. NOTE: the author of the LZO algorithms says the Linux kernel is *not* affected; media hype. (CVE-2014-4608)

- The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in both arguments to the pivot_root system call.

(CVE-2014-7970)

- The do_umount function in fs/namespace.c in the Linux kernel through 3.17 does not require the CAP_SYS_ADMIN capability for do_remount_sb calls that change the root filesystem to read-only, which allows local users to cause a denial of service (loss of writability) by making certain unshare system calls, clearing the / MNT_LOCKED flag, and making an MNT_FORCE umount system call. (CVE-2014-7975)

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

### See Also

https://ubuntu.com/security/notices/USN-2420-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

4.4

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 | 68214 |
| BID | 70314 |
| BID | 70319 |
| BID | 70691 |
| CVE | CVE-2014-3690 |
| CVE | CVE-2014-4608 |
| CVE | CVE-2014-7970 |
| CVE | CVE-2014-7975 |
| XREF | USN:2420-1 |

Plugin Information

Published: 2014/11/25, Modified: 2024/01/09

Plugin Output

tcp/0

## 81569 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2516-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2516-1 advisory.

- arch/x86/kernel/tls.c in the Thread Local Storage (TLS) implementation in the Linux kernel through 3.18.1 allows local users to bypass the espfix protection mechanism, and consequently makes it easier for local users to bypass the ASLR protection mechanism, via a crafted application that makes a set_thread_area system call and later reads a 16-bit value. (CVE-2014-8133)

- net/netfilter/nf_conntrack_proto_generic.c in the Linux kernel before 3.18 generates incorrect conntrack entries during handling of certain iptables rule sets for the SCTP, DCCP, GRE, and UDP-Lite protocols, which allows remote attackers to bypass intended access restrictions via packets with disallowed port numbers. (CVE-2014-8160)

- The d_walk function in fs/dcache.c in the Linux kernel through 3.17.2 does not properly maintain the semantics of rename_lock, which allows local users to cause a denial of service (deadlock and system hang) via a crafted application. (CVE-2014-8559)

- The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in certain namespace scenarios, which allows local users to bypass intended file permissions by leveraging a POSIX ACL containing an entry for the group category that is more restrictive than the entry for the other category, aka a negative groups issue, related to kernel/groups.c, kernel/uid16.c, and kernel/user_namespace.c. (CVE-2014-8989)

- The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel through 3.18.1 does not ensure that Thread Local Storage (TLS) descriptors are loaded before proceeding with other steps, which makes it easier for local users to bypass the ASLR protection mechanism via a crafted application that reads a TLS base address. (CVE-2014-9419)

- The rock_continue function in fs/isofs/rock.c in the Linux kernel through 3.18.1 does not restrict the number of Rock Ridge continuation entries, which allows local users to cause a denial of service (infinite loop, and system crash or hang) via a crafted iso9660 image. (CVE-2014-9420)

- The batadv_frag_merge_packets function in net/batman-adv/fragmentation.c in the B.A.T.M.A.N.

implementation in the Linux kernel through 3.18.1 uses an incorrect length field during a calculation of an amount of memory, which allows remote attackers to cause a denial of service (mesh-node system crash) via fragmented packets. (CVE-2014-9428)

- Race condition in the key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 3.18.2 allows local users to cause a denial of service (memory corruption or panic) or possibly have unspecified other impact via keyctl commands that trigger access to a key structure member during garbage collection of a key. (CVE-2014-9529)

- The parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel before 3.18.2 does not validate a length value in the Extensions Reference (ER) System Use Field, which allows local users to obtain sensitive information from kernel memory via a crafted iso9660 image. (CVE-2014-9584)

- The vdso_addr function in arch/x86/vdso/vma.c in the Linux kernel through 3.18.2 does not properly choose memory locations for the vDSO area, which makes it easier for local users to bypass the ASLR protection mechanism by guessing a location at the end of a PMD. (CVE-2014-9585)

- Off-by-one error in the ecryptfs_decode_from_filename function in fs/ecryptfs/crypto.c in the eCryptfs subsystem in the Linux kernel before 3.18.2 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted filename. (CVE-2014-9683)

- The em_sysenter function in arch/x86/kvm/emulate.c in the Linux kernel before 3.18.5, when the guest OS lacks SYSENTER MSR initialization, allows guest OS users to gain guest OS privileges or cause a denial of service (guest OS crash) by triggering use of a 16-bit code segment for emulation of a SYSENTER instruction. (CVE-2015-0239)

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

See Also

https://ubuntu.com/security/notices/USN-2516-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 70854 |

| | |
|---|---|
| BID | 71154 |
| BID | 71684 |
| BID | 71717 |
| BID | 71794 |
| BID | 71847 |
| BID | 71880 |
| BID | 71883 |
| BID | 71990 |
| BID | 72061 |
| BID | 72643 |
| BID | 72842 |
| CVE | CVE-2014-8133 |
| CVE | CVE-2014-8160 |
| CVE | CVE-2014-8559 |
| CVE | CVE-2014-8989 |
| CVE | CVE-2014-9419 |
| CVE | CVE-2014-9420 |
| CVE | CVE-2014-9428 |
| CVE | CVE-2014-9529 |
| CVE | CVE-2014-9584 |
| CVE | CVE-2014-9585 |
| CVE | CVE-2014-9683 |
| CVE | CVE-2015-0239 |
| XREF | USN:2516-1 |

## Plugin Information

Published: 2015/02/27, Modified: 2024/01/09

## Plugin Output

tcp/0

## 84614 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2663-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2663-1 advisory.

- The Btrfs implementation in the Linux kernel before 3.19 does not ensure that the visible xattr state is consistent with a requested replacement, which allows local users to bypass intended ACL settings and gain privileges via standard filesystem operations (1) during an xattr-replacement time window, related to a race condition, or (2) after an xattr-replacement attempt that fails because the data does not fit.

(CVE-2014-9710)

- Race condition in the handle_to_path function in fs/fhandle.c in the Linux kernel through 3.19.1 allows local users to bypass intended size restrictions and trigger read operations on additional memory locations by changing the handle_bytes value of a file handle during the execution of this function.

(CVE-2015-1420)

- Integer signedness error in the oz_hcd_get_desc_cnf function in drivers/staging/ozwpan/ozhcd.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted packet. (CVE-2015-4001)

- drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 does not ensure that certain length values are sufficiently large, which allows remote attackers to cause a denial of service (system crash or large loop) or possibly execute arbitrary code via a crafted packet, related to the (1) oz_usb_rx and (2) oz_usb_handle_ep_data functions. (CVE-2015-4002)

- The oz_usb_handle_ep_data function in drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via a crafted packet. (CVE-2015-4003)

- The udf_read_inode function in fs/udf/inode.c in the Linux kernel before 3.19.1 does not validate certain length values, which allows local users to cause a denial of service (incorrect data representation or integer overflow, and OOPS) via a crafted UDF filesystem. (CVE-2015-4167)

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

### See Also

https://ubuntu.com/security/notices/USN-2663-1

### Solution

Update the affected kernel package.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| BID | 73308 |
| CVE | CVE-2014-9710 |
| CVE | CVE-2015-1420 |
| CVE | CVE-2015-4001 |
| CVE | CVE-2015-4002 |
| CVE | CVE-2015-4003 |
| CVE | CVE-2015-4167 |
| XREF | USN:2663-1 |

Plugin Information

Published: 2015/07/08, Modified: 2024/01/09

Plugin Output

tcp/0

## 86190 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2748-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2748-1 advisory.

- The get_bitmap_file function in drivers/md/md.c in the Linux kernel before 4.1.6 does not initialize a certain bitmap data structure, which allows local users to obtain sensitive information from kernel memory via a GET_BITMAP_FILE ioctl call. (CVE-2015-5697)

- The vhost_dev_ioctl function in drivers/vhost/vhost.c in the Linux kernel before 4.1.5 allows local users to cause a denial of service (memory consumption) via a VHOST_SET_LOG_FD ioctl call that triggers permanent file-descriptor allocation. (CVE-2015-6252)

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

### See Also

https://ubuntu.com/security/notices/USN-2748-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2015-5697 |
| CVE | CVE-2015-6252 |
| XREF | USN:2748-1 |

## Plugin Information

Published: 2015/09/29, Modified: 2024/01/09

## Plugin Output

tcp/0

## 86785 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2794-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2794-1 advisory.

- The prepend_path function in fs/dcache.c in the Linux kernel before 4.2.4 does not properly handle rename actions inside a bind mount, which allows local users to bypass an intended container protection mechanism by renaming a directory, related to a double-chroot attack. (CVE-2015-2925)

- drivers/usb/serial/whiteheat.c in the Linux kernel before 4.2.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted USB device. NOTE: this ID was incorrectly used for an Apache Cordova issue that has the correct ID of CVE-2015-8320. (CVE-2015-5257)

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

### See Also

https://ubuntu.com/security/notices/USN-2794-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2015-2925 |
| CVE | CVE-2015-5257 |
| XREF | USN:2794-1 |

## Plugin Information

Published: 2015/11/06, Modified: 2024/01/09

## Plugin Output

tcp/0

## 87169 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2823-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2823-1 advisory.

- The sctp_init function in net/sctp/protocol.c in the Linux kernel before 4.2.3 has an incorrect sequence of protocol-initialization steps, which allows local users to cause a denial of service (panic or memory corruption) by creating SCTP sockets before all of the steps have finished. (CVE-2015-5283)

- The key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 4.2.6 allows local users to cause a denial of service (OOPS) via crafted keyctl commands. (CVE-2015-7872)

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

### See Also

https://ubuntu.com/security/notices/USN-2823-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-5283 |
| CVE | CVE-2015-7872 |
| XREF | USN:2823-1 |

Plugin Information

Published: 2015/12/02, Modified: 2024/01/09

Plugin Output

tcp/0

## 88519 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2887-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2887-1 advisory.

- Use-after-free vulnerability in net/unix/af_unix.c in the Linux kernel before 4.3.3 allows local users to bypass intended AF_UNIX socket permissions or cause a denial of service (panic) via crafted epoll_ctl calls. (CVE-2013-7446)

- arch/x86/kvm/x86.c in the Linux kernel before 4.4 does not reset the PIT counter values during state restoration, which allows guest OS users to cause a denial of service (divide-by-zero error and host OS crash) via a zero value, related to the kvm_vm_ioctl_set_pit and kvm_vm_ioctl_set_pit2 functions.

(CVE-2015-7513)

- Race condition in the rds_sendmsg function in net/rds/sendmsg.c in the Linux kernel before 4.3.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6937. (CVE-2015-7990)

- fs/btrfs/inode.c in the Linux kernel before 4.3.3 mishandles compressed inline extents, which allows local users to obtain sensitive pre-truncation information from a file via a clone action. (CVE-2015-8374)

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

### See Also

https://ubuntu.com/security/notices/USN-2887-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2013-7446 |
| CVE | CVE-2015-7513 |
| CVE | CVE-2015-7990 |
| CVE | CVE-2015-8374 |
| XREF | USN:2887-1 |

Plugin Information

Published: 2016/02/02, Modified: 2024/01/09

Plugin Output

tcp/0

## 92862 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3052-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3052-1 advisory.

- The key_reject_and_link function in security/keys/key.c in the Linux kernel through 4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command. (CVE-2016-4470)

- The tipc_nl_compat_link_dump function in net/tipc/netlink_compat.c in the Linux kernel through 4.6.3 does not properly copy a certain string, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message. (CVE-2016-5243)

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

### See Also

https://ubuntu.com/security/notices/USN-3052-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-4470 |
| CVE | CVE-2016-5243 |
| XREF | USN:3052-1 |

Plugin Information

Published: 2016/08/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 93954 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3098-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3098-1 advisory.

- Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a double fetch vulnerability. (CVE-2016-6136)

- Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a double fetch vulnerability. (CVE-2016-6480)

- The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option.

(CVE-2016-6828)

- The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666. (CVE-2016-7039)

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

### See Also

https://ubuntu.com/security/notices/USN-3098-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-6136 |
| CVE | CVE-2016-6480 |
| CVE | CVE-2016-6828 |
| CVE | CVE-2016-7039 |
| XREF | USN:3098-1 |

Plugin Information

Published: 2016/10/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 95993 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3160-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3160-1 advisory.

- fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a loop that triggers exponential growth in the number of mounts. (CVE-2016-6213)

- Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/*/environ file during a process-setup time interval in which environment-variable copying is incomplete. (CVE-2016-7916)

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

### See Also

https://ubuntu.com/security/notices/USN-3160-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-6213 |
| CVE | CVE-2016-7916 |
| XREF | USN:3160-1 |

Plugin Information

Published: 2016/12/21, Modified: 2024/01/09

Plugin Output

tcp/0

## 103780 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3445-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3445-1 advisory.

- drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remote attackers to execute arbitrary code via crafted fragmented packets. (CVE-2016-8633)

- The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path. (CVE-2017-14106)

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

### See Also

https://ubuntu.com/security/notices/USN-3445-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-8633 |
| CVE | CVE-2017-14106 |
| XREF | USN:3445-1 |

Plugin Information

Published: 2017/10/11, Modified: 2024/01/09

Plugin Output

tcp/0

## 106272 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3542-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3542-1 advisory.

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

(CVE-2017-5715)

- Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

(CVE-2017-5753)

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

### See Also

https://ubuntu.com/security/notices/USN-3542-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

8.4

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2017-5715 |
| CVE | CVE-2017-5753 |
| XREF | USN:3542-1 |
| XREF | IAVA:2018-A-0020 |

Exploitable With

CANVAS (true)

Plugin Information

Published: 2018/01/23, Modified: 2024/01/09

Plugin Output

tcp/0

## 111753 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-3742-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3742-1 advisory.

- The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /proc/$PID/timers is read). This allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIMERS and CONFIG_CHECKPOINT_RESTORE).

(CVE-2017-18344)

- Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis. (CVE-2018-3620)

- Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis. (CVE-2018-3646)

- Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service. (CVE-2018-5390)

- The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size. (CVE-2018-5391)

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

### See Also

https://ubuntu.com/security/notices/USN-3742-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-18344 |
| CVE | CVE-2018-3620 |
| CVE | CVE-2018-3646 |
| CVE | CVE-2018-5390 |
| CVE | CVE-2018-5391 |
| XREF | USN:3742-1 |

Exploitable With

CANVAS (true)

Plugin Information

Published: 2018/08/15, Modified: 2024/01/09

Plugin Output

tcp/0

## 81646 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities regression (USN-2516-3)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2516-3 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-2516-3

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### VPR Score

6.7

### References

| | |
|---|---|
| BID | 70854 |
| BID | 71154 |
| BID | 71684 |
| BID | 71717 |
| BID | 71794 |
| BID | 71847 |
| BID | 71880 |
| BID | 71883 |
| BID | 71990 |
| BID | 72061 |
| BID | 72643 |
| BID | 72842 |
| CVE | CVE-2014-8133 |
| CVE | CVE-2014-8160 |
| CVE | CVE-2014-8559 |

| | |
|---|---|
| CVE | CVE-2014-8989 |
| CVE | CVE-2014-9419 |
| CVE | CVE-2014-9420 |
| CVE | CVE-2014-9428 |
| CVE | CVE-2014-9529 |
| CVE | CVE-2014-9584 |
| CVE | CVE-2014-9585 |
| CVE | CVE-2014-9683 |
| CVE | CVE-2015-0239 |
| XREF | USN:2516-3 |

## Plugin Information

Published: 2015/03/05, Modified: 2024/01/09

## Plugin Output

tcp/0

## 85509 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2716-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2716-1 advisory.

- Race condition in net/sctp/socket.c in the Linux kernel before 4.1.2 allows local users to cause a denial of service (list corruption and panic) via a rapid series of system calls related to sockets, as demonstrated by setsockopt calls. (CVE-2015-3212)

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

### See Also

https://ubuntu.com/security/notices/USN-2716-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-3212 |
| XREF | USN:2716-1 |

Plugin Information

Published: 2015/08/18, Modified: 2024/01/09

Plugin Output

tcp/0

## 86811 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-2801-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2801-1 advisory.

- The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #AC (aka Alignment Check) exceptions, related to svm.c and vmx.c. (CVE-2015-5307)

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

### See Also

https://ubuntu.com/security/notices/USN-2801-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-5307 |
| XREF | USN:2801-1 |

Plugin Information

Published: 2015/11/10, Modified: 2024/01/09

Plugin Output

tcp/0

## 99655 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3264-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3264-1 advisory.

- Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state. (CVE-2017-5986)

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

### See Also

https://ubuntu.com/security/notices/USN-3264-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2017-5986 |
| XREF | USN:3264-1 |

Plugin Information

Published: 2017/04/25, Modified: 2024/01/09

Plugin Output

tcp/0

## 100251 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3290-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3290-1 advisory.

- The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c. (CVE-2016-8645)

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

### See Also

https://ubuntu.com/security/notices/USN-3290-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2016-8645 |
| XREF | USN:3290-1 |

Plugin Information

Published: 2017/05/17, Modified: 2024/01/09

Plugin Output

tcp/0

## 105727 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3524-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3524-1 advisory.

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. (CVE-2017-5754)

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

### See Also

https://ubuntu.com/security/notices/USN-3524-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

8.1

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2017-5754 |
| XREF | USN:3524-1 |
| XREF | IAVA:2018-A-0019 |

## Plugin Information

Published: 2018/01/10, Modified: 2024/01/09

## Plugin Output

tcp/0

## 107293 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3594-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3594-1 advisory.

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

(CVE-2017-5715)

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

### See Also

https://ubuntu.com/security/notices/USN-3594-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.6

### 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

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2017-5715 |
| XREF | USN:3594-1 |
| XREF | IAVA:2018-A-0020 |

## Plugin Information

Published: 2018/03/12, Modified: 2024/01/09

## Plugin Output

tcp/0

## 122813 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-3908-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3908-1 advisory.

- In PolicyKit (aka polkit) 0.115, the start time protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c. (CVE-2019-6133)

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

### See Also

https://ubuntu.com/security/notices/USN-3908-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2019-6133 |
| XREF | USN:3908-1 |

Plugin Information

Published: 2019/03/13, Modified: 2024/01/09

Plugin Output

tcp/0

## 190818 - Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-6645-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6645-1 advisory.

- A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow. (CVE-2023-7192)

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

### See Also

https://ubuntu.com/security/notices/USN-6645-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-7192 |
| XREF | USN:6645-1 |

Plugin Information

Published: 2024/02/20, Modified: 2024/02/20

Plugin Output

tcp/0

## 81590 - Ubuntu 14.04 LTS : Linux kernel vulnerability regression (USN-2516-2)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-2516-2 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-2516-2

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### VPR Score

6.7

### References

| | |
|---|---|
| BID | 70854 |
| BID | 71154 |
| BID | 71684 |
| BID | 71717 |
| BID | 71794 |
| BID | 71847 |
| BID | 71880 |
| BID | 71883 |
| BID | 71990 |
| BID | 72061 |
| BID | 72643 |
| BID | 72842 |
| CVE | CVE-2014-8133 |
| CVE | CVE-2014-8160 |
| CVE | CVE-2014-8559 |

| | |
|---|---|
| CVE | CVE-2014-8989 |
| CVE | CVE-2014-9419 |
| CVE | CVE-2014-9420 |
| CVE | CVE-2014-9428 |
| CVE | CVE-2014-9529 |
| CVE | CVE-2014-9584 |
| CVE | CVE-2014-9585 |
| CVE | CVE-2014-9683 |
| CVE | CVE-2015-0239 |
| XREF | USN:2516-2 |

## Plugin Information

Published: 2015/03/02, Modified: 2024/01/09

## Plugin Output

tcp/0

## 125145 - Ubuntu 14.04 LTS : linux vulnerabilities (USN-3983-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

### Synopsis

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

### Description

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Giorgi Maisuradze, Dan Horea Lutas, Andrei Lutas, Volodymyr Pikhur, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Moritz Lipp, Michael Schwarz, and Daniel Gruss discovered that memory previously stored in microarchitectural fill buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information.

(CVE-2018-12130)

Brandon Falk, Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that memory previously stored in microarchitectural load ports of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12127)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Marina Minkin, Daniel Moghimi, Moritz Lipp, Michael Schwarz, Jo Van Bulck, Daniel Genkin, Daniel Gruss, Berk Sunar, Frank Piessens, and Yuval Yarom discovered that memory previously stored in microarchitectural store buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12126)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Volodrmyr Pikhur, Moritz Lipp, Michael Schwarz, Daniel Gruss, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that uncacheable memory previously stored in microarchitectural buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11091).

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/3983-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-12126 |
| CVE | CVE-2018-12127 |
| CVE | CVE-2018-12130 |
| CVE | CVE-2019-11091 |
| XREF | USN:3983-1 |
| XREF | CEA-ID:CEA-2019-0547 |
| XREF | CEA-ID:CEA-2019-0324 |

Plugin Information

Published: 2019/05/15, Modified: 2024/05/28

Plugin Output

tcp/0

## 57640 - Web Application Information Disclosure

### Synopsis

The remote web application discloses path information.

### Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

### Solution

Filter error messages containing path information.

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2012/01/25, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
The request GET /drupal/?pass=%00ftcigl HTTP/1.1
Host: 10.0.2.9
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*


produces the following path information :
<h2 class="element-invisible">Error message</h2>
<ul>
<li><em class="placeholder">Warning</em>: Illegal string offset 'field'
in <em class="placeholder">DatabaseCondition-&gt;__clone()</em> (line <e
m class="placeholder">1817</em> of <em class="placeholder">/var/www/html
/drupal/includes/database/query.inc</em>).</li>
<li><em class="placeholder">Warning</em>: Illegal string offset 'f [...]
</ul>
```

```
The request GET /drupal/?form_build_id=%00ftcigl HTTP/1.1
Host: 10.0.2.9
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*


produces the following path information :
<h2 class="element-invisible">Error message</h2>
<ul>
<li><em class="placeholder">Warning</em>: Illegal string offset 'field'
in <em class="placeholder">DatabaseCondition-&gt;__clone()</em> (line <e
m class="placeholder">1817</em> of <em class="placeholder">/var/www/html
/drupal/includes/database/query.inc</em>).</li>
<li><em class="placeholder">Warning</em>: Illegal string offset 'f [...]
</ul>

The request POST /drupal/ HTTP/1.1
Host: 10.0.2.9
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 147
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
destination=node&form_build_id=form-d8LdjYn0RUG0TOJvGyqs1cbfT5g2VZRXrV9DuvGs4YA&q=rss.xml&pass
 [...]
```

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

### See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

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

### Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:693 |

## Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

## Plugin Output

tcp/80/www

## 10114 - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

### Risk Factor

Low

### VPR Score

4.2

### 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: 2024/05/03

### Plugin Output

icmp/0

```
The difference between the local and remote clocks is 1 second.
```

## 76791 - PHP 5.4.x < 5.4.31 CLI Server 'header' DoS

### Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

### Description

According to its banner, the version of PHP 5.4.x in use on the remote web server is a version prior to 5.4.31. It is, therefore, affected by a denial of service vulnerability that affects the built-in command line development server.

The function 'sapi_cli_server_send_headers' in the file 'sapi/cli/php_cli_server.c' contains an error that does not properly handle an empty 'header' parameter and could allow denial of service attacks.

Note that this issue affects only the built-in command line development server.

Further note that Nessus has not attempted to exploit this issue, but has instead relied only on the application's self-reported version number.

### See Also

http://www.php.net/ChangeLog-5.php#5.4.31

https://bugs.php.net/bug.php?id=66830

### Solution

Upgrade to PHP version 5.4.31 or later.

### Risk Factor

Low

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2014/07/25, Modified: 2024/05/31

### Plugin Output

tcp/80/www

## 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

3.6

### 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

## 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

## 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

## 87466 - Ubuntu 14.04 LTS : Linux kernel vulnerabilities (USN-2841-1)

### Synopsis

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

### Description

The remote Ubuntu 14.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-2841-1 advisory.

- The slhc_init function in drivers/net/slip/slhc.c in the Linux kernel through 4.2.3 does not ensure that certain slot numbers are valid, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted PPPIOCSMAXCID ioctl call. (CVE-2015-7799)

- The dgnc_mgmt_ioctl function in drivers/staging/dgnc/dgnc_mgmt.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application. (CVE-2015-7885)

- The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #DB (aka Debug) exceptions, related to svm.c. (CVE-2015-8104)

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

### See Also

https://ubuntu.com/security/notices/USN-2841-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-7799 |
| CVE | CVE-2015-7885 |
| CVE | CVE-2015-8104 |
| XREF | USN:2841-1 |

Plugin Information

Published: 2015/12/17, Modified: 2024/01/09

Plugin Output

tcp/0

## 42057 - Web Server Allows Password Auto-Completion

### Synopsis

The 'autocomplete' attribute is not disabled on password fields.

### Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

### Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

### Risk Factor

Low

### Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

### Plugin Output

tcp/80/www

```
Page : /drupal/
Destination Page: /drupal/?q=node&destination=node

Page : /payroll_app.php
Destination Page: /payroll_app.php

Page : /phpmyadmin/
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/url.php
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/index.php
Destination Page: /phpmyadmin/index.php
```

## 26194 - Web Server Transmits Cleartext Credentials

### Synopsis

The remote web server might transmit credentials in cleartext.

### Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

### Solution

Make sure that every sensitive form transmits content over HTTPS.

### Risk Factor

Low

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:523 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

### Plugin Output

tcp/80/www

## 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: 2022/03/21

### Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 14.04 (trusty)
```

## 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: 2024/06/21

### Plugin Output

tcp/0

## 142640 - Apache HTTP Server Site Enumeration

### Synopsis

The remote host is hosting websites using Apache HTTP Server.

### Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

### See Also

https://httpd.apache.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/11/09, Modified: 2024/05/20

### Plugin Output

tcp/0

## 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

## 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

## 39519 - Backported Security Patch Detection (FTP)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote FTP 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/21/ftp

## 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

## 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

## 47830 - CGI Generic Injectable Parameter

### Synopsis

Some CGIs are candidate for extended injection tests.

### Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

### Solution

n/a

### Risk Factor

None

### References

XREF CWE:86

### Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'db' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?db=%00ftcigl
+ The 'lang' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?lang=ftcigl
+ The 'table' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?table=%00ftcigl
+ The 'pma_username' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?pma_username=%00ftcigl
+ The 'db' parameter of the /phpmyadmin/index.php CGI :
```

```
/phpmyadmin/index.php?db=%00ftcigl&lang=&token=69830204c8eac460ae4129138
9c9868c&table=&server=1&pma_username=&pma_password=
+ The 'lang' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?db=&lang=ftcigl&token=69830204c8eac460ae41291389c9
868c&table=&server=1&pma_username=&pma_password=
+ The 'table' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?db=&lang=&token=69830204c8eac460ae41291389c9868c&t
able=%00ftcigl&server=1&pma_username=&pma_password=
+ The 'pma_username' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?db=&lang=&token=69830204c8eac460ae41291389c9868c&t
able=&server=1&pma_username=%00ftcigl&pma_password=
+ The 'destination' parameter of the /drupal/ CGI :

/drupal/?destination=%00ftcigl
+ The 'form_build_id' parameter of the /drupal/ CGI :

/drupal/?form_build_id=%00ftcigl
+ The 'q' parameter of the /drupal/ CGI :

/drupal/?q=%00ftcigl
+ The 'pass' parameter of the /drupal/ CGI :

/drupal/?pass=%00ftcigl
+ The 'op' parameter of the /drupal/ CGI :

/drupal/?op=%00ftcigl
+ The 'name' parameter of the /drupal/ CGI :

/drupal/?name=%00ftcigl
+ The 'form_id' parameter of the /drupal/ CGI :

/drupal/?form_id=%00ftcigl
+ The 'q' parameter of the /drupal/ CGI :

/drupal/?destination=node&form_build_id=form-d8LdjYn0RUG0TOJvGyqs1cbfT5g
2VZRXrV9DuvGs4YA&q=%00ftcigl&pass=&op=Log%20in&name=&form_id=user_login_
block
Clicking directly on these URLs should exhibit the issue :
(you will probably nee [...]
```

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=13         SP=13        AP=37        SC=2         AC=58

SQL injection                            : S=700        SP=700       AP=2016      SC=0
 AC=5180
unseen parameters                        : S=875        SP=875       AP=2520      SC=0
 AC=6475
local file inclusion                     : S=100        SP=100       AP=288       SC=0
 AC=740
web code injection                       : S=25         SP=25        AP=72        SC=0
 AC=185
XML injection                            : S=25         SP=25        AP=72        SC=0
 AC=185
format string                            : S=50         SP=50        AP=144       SC=0
 AC=370
script injection                         : S=13         SP=13        AP=37        SC=2         AC=58

cross-site scripting (comprehensive test): S=425        SP=425       AP=1224      SC=0
 AC=3145
```

```
injectable parameter                      : S=50         SP=50        AP=144       SC=0
 AC=370
cross-site scripting (extended patterns) : S=78         SP=78        AP=222       SC=12
 AC=348
directory traversal (write access)       : S=50         SP=50        AP=144       SC=0
 AC=370
SSI injection                             : S=75         SP=75        AP=216       SC=0
 AC=555
header injection                          : S=26         SP=26        AP=74        SC=4
 AC=116
HTML injection                            : S=65         SP=65        AP=185       SC=10
 AC=290
directory traversal                       : S=725        SP=725       AP=2088      SC=0
 AC=5365
arbitrary command execution (time based) : S=150        SP=150       AP=432       SC=0
 AC=1110
persistent XSS                           [...]
```

## 39470 - CGI Generic Tests Timeout

### Synopsis

Some generic CGI attacks ran out of time.

### Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

### Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

### Risk Factor

None

### Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- SQL injection
- directory traversal (extended test)
- uncontrolled redirection
- local file inclusion
- blind SQL injection (time based)
- arbitrary command execution
- directory traversal
- cross-site scripting (extended patterns)

The following tests were interrupted and did not report all possible flaws :
- cross-site scripting (comprehensive test)
- blind SQL injection
```

## 200242 - Chef Infra Client Installed (Unix)

### Synopsis

Chef Infra Client is installed on the remote Unix host.

### Description

Chef Infra Client is installed on the remote Unix host.

### See Also

https://community.chef.io/downloads/tools/infra-client

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

## 45590 - Common Platform Enumeration (CPE)

### Synopsis

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

### Description

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

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

### See Also

http://cpe.mitre.org/

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/21, Modified: 2024/06/20

### Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:14.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:chef:chef:13.8.5 -> Chef
  cpe:/a:docker:docker:18.06.1-ce -> Docker
  cpe:/a:drupal:drupal:7.5 -> Drupal
  cpe:/a:eclipse:jetty:8.1.7 -> Eclipse Jetty
  cpe:/a:gnupg:libgcrypt:1.5.3 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.35.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.35.0 -> Haxx libcurl
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:mysql:mysql:5.5.62-0ubuntu0.14.04.1_ -> MySQL MySQL
  cpe:/a:nodejs:node.js:4.9.1 -> Nodejs Node.js
```

```
cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:6.6.1p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1f -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.2n -> OpenSSL Project OpenSSL
cpe:/a:php:php:5.4.5 -> PHP PHP
cpe:/a:phpmyadmin:phpmyadmin:3.5.8 -> phpMYAdmin
cpe:/a:samba:samba -> Samba Samba
cpe:/a:samba:samba:4.3.11 -> Samba Samba
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tukaani:xz:5.1.1al -> Tukaani XZ
cpe:/a:tukaani:xz:5.2.3 -> Tukaani XZ
cpe:/a:vim:vim:7.4 -> Vim
cpe:/a:vmware:open_vm_tools:9.4.0 -> VMware Open VM Tools
x-cpe:/a:java:jre:6.0.41.41
```

## 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: 2024/06/21

### Plugin Output

tcp/0

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2024/06/14

### Plugin Output

tcp/0

```
Hostname : metasploitable3-ub1404
  metasploitable3-ub1404 (hostname command)
```

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

### Plugin Output

tcp/0

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

## 159488 - Docker Installed (Linux)

### Synopsis

Docker was detected on the remote host.

### Description

A container virtualization suite is installed on the remote host.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/04, Modified: 2024/06/21

### Plugin Output

tcp/0

## 18638 - Drupal Software Detection

### Synopsis

A content management system is running on the remote web server.

### Description

Drupal, an open source content management system written in PHP, is running on the remote web server.

### See Also

https://www.drupal.org/

### Solution

Ensure that the use of this software aligns with your organization's security and acceptable use policies.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0586 |

### Plugin Information

Published: 2005/07/07, Modified: 2023/05/24

### Plugin Output

tcp/80/www

## 194915 - Eclipse Jetty Web Server Detection

### Synopsis

The Eclipse Jetty web server was detected on the remote host.

### Description

The Eclipse Jetty web server was detected on the remote host.

### See Also

https://eclipse.dev/jetty/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/05/02, Modified: 2024/05/20

### Plugin Output

tcp/0

## 19689 - Embedded Web Server Detection

### Synopsis

The remote web server is embedded.

### Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

### Plugin Output

tcp/631/www

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

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

### Description

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

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2024/02/05

### Plugin Output

tcp/0

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

 - 172.17.0.1 (on interface docker0)
 - 10.0.2.9 (on interface eth0)
 - 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: 2022/02/23

### Plugin Output

tcp/0

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

 - fe80::42:5dff:feb4:5086 (on interface docker0)
 - fe80::a00:27ff:fe0e:2bcc (on interface eth0)
 - ::1 (on interface lo)
 - fe80::6417:fcff:fe53:af9b (on interface veth48c6ba7)
```

## 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

## 170170 - Enumerate the Network Interface configuration via SSH

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/01/19, Modified: 2023/11/17

### Plugin Output

tcp/0

## 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

## 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: 2024/06/21

### Plugin Output

tcp/0

## 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 :

08:00:27:0E:2B:CC : 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: 2020/05/13

### Plugin Output

tcp/0

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/80/www

```
3 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://drupal.org                       - /drupal/
https://github.com/rapid7/metasploitable3/wiki - /drupal/
https://github.com/rapid7/metasploitable3/wiki/Tips-and-Tricks - /drupal/
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/3500/www

```
4 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://api.rubyonrails.org/             - /
http://guides.rubyonrails.org/          - /
http://www.ruby-doc.org/core/           - /
http://www.ruby-doc.org/stdlib/         - /
```

## 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 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.9]
```

## 69826 - HTTP Cookie 'secure' Property Transport Mismatch

### Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

### Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

### See Also

https://tools.ietf.org/html/rfc6265

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

### Plugin Output

tcp/631/www

## 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 COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND
    PROPPATCH TRACE UNLOCK are allowed on :

    /uploads

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /drupal/misc
    /drupal/misc/farbtastic
    /drupal/misc/ui
    /drupal/misc/ui/images
    /icons
    /phpmyadmin/themes
    /phpmyadmin/themes/original
    /phpmyadmin/themes/original/css
    /phpmyadmin/themes/original/img
    /phpmyadmin/themes/original/img/pmd
    /phpmyadmin/themes/original/jquery
    /phpmyadmin/themes/original/jquery/images
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/css


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 COPY DELETE GET HEAD 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 :

    /uploads

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /chat
    /drupal
    /drupal/misc
    /drupal/misc/farbtastic
    /drupal/misc/ui
    /drupal/misc/ui/images
    /icons
    /phpmyadmin
    /phpmyadmin/themes
    /phpmyadmin/themes/original
    /phpmyadmin/themes/original/css
    /phpmyadmin/themes/original/img
    /phpmyadmin/themes/original/img/pmd
    /phpmyadmin/themes/original/jquery
    /phpmyadmin/themes/original/jquery/images
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/css

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
```

```
    /uploads
```

## 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/631/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  HEAD  OPTIONS  POST  PUT GET are allowed on :

    /

Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

## 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/3500/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT 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 TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /
    //
    /rails/info

  - Invalid/unknown HTTP methods are allowed on :

    /
    //
    /rails/info
```

## 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/8080/www

```
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 TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

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

### Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

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

### Plugin Output

tcp/631/www

```
The remote web server type is :

CUPS/1.7 IPP/2.1
```

## 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/3500/www

```
The remote web server type is :

WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
```

## 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/8080/www

```
The remote web server type is :

Jetty(8.1.7.v20120910)
```

## 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: Mon, 24 Jun 2024 00:54:30 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Vary: Accept-Encoding
  Content-Length: 1346
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html;charset=UTF-8

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
```

```
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</
a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
 href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="chat/">chat/</a></
td><td align="right">2020-10-29 19:37  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="drupal/">drupal/</
a></td><td align="right">2011-07-27 20:17  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a
 href="payroll_app.php">payroll_app.php</a></td><td align="right">2020-10-29 19:37  </td><td
 align="right">1.7K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a
 href="phpmyadmin/">phpmyadmin/</a></td><td align="right">2013-04-08 12:06  </td><td align="right">
 - </td><td> </td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.7 (Ubuntu) Server at 10.0.2.9 Port 80</address>
</body></html>
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/3500/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 : GET,HEAD,POST,OPTIONS
Headers :

  X-Frame-Options: SAMEORIGIN
  X-Xss-Protection: 1; mode=block
  X-Content-Type-Options: nosniff
  Content-Type: text/html; charset=utf-8
  Etag: W/"b56dd5f9363ed0f7bd4d11c36d9471dd"
  Cache-Control: max-age=0, private, must-revalidate
  X-Request-Id: 8f65a16f-41bc-4848-b630-0f5d9ab32f77
  X-Runtime: 0.003967
  Server: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
  Date: Mon, 24 Jun 2024 00:54:30 GMT
  Content-Length: 14935
  Connection: Keep-Alive

Response Body :

<!DOCTYPE html>
<html>
```

```
  <head>
    <title>Ruby on Rails: Welcome aboard</title>
    <style media="screen">
      body {
        margin: 0;
        margin-bottom: 25px;
        padding: 0;
        background-color: #f0f0f0;
        font-family: "Lucida Grande", "Bitstream Vera Sans", "Verdana";
        font-size: 13px;
        color: #333;
      }

      h1 {
        font-size: 28px;
        color: #000;
      }

      a  {color: #03c}

      a:hover {
        background-color: #03c;
        color: white;
        text-decoration: none;
      }

      #page {
        background-color: #f0f0f0;
        width: 750px;
        margin: 0;
        margin-left: auto;
        margin-right: auto;
      }

      #content {
        float: left;
        background-color: white;
        border: 3px solid #aaa;
        border-top: none;
        padding: 25px;
        width: 500px;
      }

      #sidebar {
        float: right;
        width: 175px;
      }

      #footer {
        clear: both;
      }

      #header, #about, #getting-started {
        padding-left: 75px;
        padding-right: 30px;
      }

      #header {
        background-image: url(
t5Sr9aurl6qO013Z9/DEoJh18gZQGAUxPHIyQHH7eioZ8bjnAFHZ0RndNxxRBhGcUbxoKIHBkTEcUYREIHIGpKQjUDS6 [...]
```

## 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/8080/www

```
Response Code : HTTP/1.1 404 Not Found

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

  Date: Mon, 24 Jun 2024 00:54:30 GMT
  Content-Type: text/html
  Content-Length: 795
  Connection: close
  Server: Jetty(8.1.7.v20120910)

Response Body :
```

## 171410 - IP Assignment Method Detection

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2024/06/21

### Plugin Output

tcp/0

## 118237 - JAR File Detection for Linux/UNIX

### Synopsis

Detected JAR files on the host.

### Description

The host contains JAR files, Java Archive files.

Note that this plugin only detects JAR files in commonly used installation directories or a user specified search path.

### See Also

https://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/22, Modified: 2024/06/21

### Plugin Output

tcp/0

## 147817 - Java Detection and Identification (Linux / Unix)

### Synopsis

Java is installed on the remote Linux / Unix host.

### Description

One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- This plugin attempts to detect Oracle and non-Oracle JRE instances such as Zulu Java, Amazon Corretto, AdoptOpenJDK, IBM Java, etc

- To discover instances of JRE that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

### See Also

https://en.wikipedia.org/wiki/Java_(software_platform)

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0690 |

### Plugin Information

Published: 2021/03/16, Modified: 2024/06/21

### Plugin Output

tcp/0

## 151883 - Libgcrypt Installed (Linux/UNIX)

### Synopsis

Libgcrypt is installed on this host.

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/07/21, Modified: 2024/06/21

### Plugin Output

tcp/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

## 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

## 95928 - Linux User List Enumeration

### Synopsis

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

### Description

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

### Solution

None

### Risk Factor

None

### Plugin Information

Published: 2016/12/19, Modified: 2024/03/13

### Plugin Output

tcp/0

## 42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

### Synopsis

It is possible to obtain the network name of the remote host.

### Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/11/06, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 METASPLOITABLE3-UB1404 = Computer name
 METASPLOITABLE3-UB1404 = Workgroup / Domain name
```

## 17651 - Microsoft Windows SMB : Obtains the Password Policy

### Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

### Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

### Plugin Output

tcp/445/cifs

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

## 10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

### Synopsis

It is possible to obtain the host SID for the remote host.

### Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

### See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

### Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

### Risk Factor

None

### Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

### Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-3430637069-1686740736-3619866930

The value of 'RestrictAnonymous' setting is : unknown
```

## 10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

### Synopsis

It was possible to obtain information about the remote operating system.

### Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

### Plugin Output

tcp/445/cifs

## 11011 - Microsoft Windows SMB Service Detection

### Synopsis

A file / print sharing service is listening on the remote host.

### Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

### Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

## 60119 - Microsoft Windows SMB Share Permissions Enumeration

### Synopsis

It was possible to enumerate the permissions of remote network shares.

### Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

### See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx

https://technet.microsoft.com/en-us/library/cc783530.aspx

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

### Plugin Output

tcp/445/cifs

```
Share path : \\METASPLOITABLE3-UB1404\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\METASPLOITABLE3-UB1404\public
Local path : C:\var\www\html\
Comment : WWW
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\METASPLOITABLE3-UB1404\IPC$
Local path : C:\tmp
Comment : IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:         YES
```

```
    FILE_GENERIC_WRITE:         YES
    FILE_GENERIC_EXECUTE:       YES
```

## 10395 - Microsoft Windows SMB Shares Enumeration

### Synopsis

It is possible to enumerate remote network shares.

### Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

### Plugin Output

tcp/445/cifs

## 100871 - Microsoft Windows SMB Versions Supported (remote check)

### Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

### Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

## 106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

### Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

### Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

### Plugin Output

tcp/445/cifs

## 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

## 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/3500/www

## 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

## 10719 - MySQL Server Detection

### Synopsis

A database server is listening on the remote port.

### Description

The remote host is running MySQL, an open source database server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0802

### Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

### Plugin Output

tcp/3306/mysql

```
The remote database access is restricted and configured to reject access
from unauthorized IPs.  Therefore it was not possible to extract its
version number.
```

## 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: 2023/10/27

### Plugin Output

tcp/0

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/06/04

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406231231
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : ejer_2_tech__unidad_1_sprint_4
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : netstat
Port range : 1-65535
Ping RTT : 150.271 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 0
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'vagrant' 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 : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/6/24 2:49 CEST
Scan duration : 3415 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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### 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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/68

```
Port 68/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### 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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/111

```
Port 111/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/111

```
Port 111/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/137

```
Port 137/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/138

```
Port 138/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/139

```
Port 139/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/631/www

```
Port 631/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/631

```
Port 631/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/851

```
Port 851/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/3306/mysql

```
Port 3306/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/3500/www

```
Port 3500/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/6667

```
Port 6667/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/6697/irc

```
Port 6697/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/8067

```
Port 8067/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/8080/www

```
Port 8080/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/35177

```
Port 35177/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/37321

```
Port 37321/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/37681

```
Port 37681/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/41781

```
Port 41781/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/51785

```
Port 51785/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/53673

```
Port 53673/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

udp/56955

```
Port 56955/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: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

### Plugin Output

tcp/57308

```
Port 57308/tcp was found to be open
```

## 178771 - Node.js Installed (Linux / UNIX)

### Synopsis

Node.js is installed on the remote Linux / UNIX host.

### Description

Node.js is installed on the remote Linux / UNIX host.

### See Also

https://nodejs.org

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/07/25, Modified: 2024/06/21

### Plugin Output

tcp/0

## 178772 - Node.js Modules Installed (Linux)

### Synopsis

Nessus was able to enumerate one or more Node.js modules installed on the remote host.

### Description

Nessus was able to enumerate one or more Node.js modules installed on the remote host.
Note that 'Perform thorough tests' may be required for an in-depth search of all Node.js modules.

### See Also

https://nodejs.org/api/modules.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/07/25, Modified: 2024/06/21

### Plugin Output

tcp/0

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.13.0-24-generic on Ubuntu 14.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.13.0-24-generic on Ubuntu 14.04
```

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

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/05/30, Modified: 2024/03/19

### 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 metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
 x86_64 x86_64 GNU/Linux

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

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 4.438953 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

## 181418 - OpenSSH Detection

### Synopsis

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

### Description

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

### See Also

https://www.openssh.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/09/14, Modified: 2024/06/21

### Plugin Output

tcp/22/ssh

## 168007 - OpenSSL Installed (Linux)

### Synopsis

OpenSSL was detected on the remote Linux host.

### Description

OpenSSL was detected on the remote Linux host.

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

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

### See Also

https://openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/11/21, Modified: 2024/06/21

### Plugin Output

tcp/0

## 48243 - PHP Version Detection

### Synopsis

It was possible to obtain the version number of the remote PHP installation.

### Description

Nessus was able to determine the version of PHP available on the remote web server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0936

### Plugin Information

Published: 2010/08/04, Modified: 2024/05/31

### Plugin Output

tcp/80/www

## 66334 - Patch Report

### Synopsis

The remote host is missing several patches.

### Description

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

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

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information

Published: 2013/07/08, Modified: 2024/06/11

### Plugin Output

tcp/0

## 45405 - Reachable IPv6 address

### Synopsis

The remote host may be reachable from the Internet.

### Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

### Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

### Risk Factor

None

### Plugin Information

Published: 2010/04/02, Modified: 2012/08/07

### Plugin Output

tcp/0

```
The following global addresss were gathered :

  - ['ipv6': fe80::42:5dff:feb4:5086]['scope': link]['prefixlen': 64]
  - ['ipv6': fe80::a00:27ff:fe0e:2bcc]['scope': link]['prefixlen': 64]
  - ['ipv6': ::1]['scope': host]['prefixlen': 128]
  - ['ipv6': fe80::6417:fcff:fe53:af9b]['scope': link]['prefixlen': 64]
```

## 10860 - SMB Use Host SID to Enumerate Local Users

### Synopsis

Nessus was able to enumerate local users.

### Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/02/13, Modified: 2023/02/28

### Plugin Output

tcp/445/cifs

```
  - nobody (id 501, Guest account)
  - chewbacca (id 1000)

Note that, in addition to the Administrator, Guest, and Kerberos
accounts, Nessus has enumerated local users with IDs between
1000 and 1200. To use a different range, edit the scan policy
and change the 'Enumerate Local Users: Start UID' and/or 'End UID'
preferences under 'Assessment->Windows' and re-run the scan. Only
UIDs between 1 and 2147483647 are allowed for this range.
```

## 174788 - SQLite Local Detection (Linux)

### Synopsis

The remote Linux host has SQLite Database software installed.

### Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

### See Also

https://www.sqlite.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/04/26, Modified: 2024/06/21

### Plugin Output

tcp/0

## 70657 - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

### Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  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 server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
```

```
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sh [...]
```

## 102094 - SSH Commands Require Privilege Escalation

### Synopsis

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

### Description

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

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0507 |

### Plugin Information

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

### Plugin Output

tcp/0

## 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: 2021/01/19

### 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: 2023/11/27

### 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

## 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: 2020/09/22

### Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
SSH supported authentication : publickey,password
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

### Plugin Output

tcp/631/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

## 45410 - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

tcp/631/www

```
The host name known by Nessus is :

  metasploitable3-ub1404

The Common Name in the certificate is :

  ubuntu
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/631/www

## 70544 - SSL Cipher Block Chaining Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

### Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

### See Also

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

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

### Plugin Output

tcp/631/www

## 21643 - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

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

### See Also

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

### Plugin Output

tcp/631/www

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

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA               0x00, 0x41        RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA               0x00, 0x84        RSA           RSA      Camellia-CBC(256)
 SHA1
```

```
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AES128-SHA                    0x00, 0x2F       RSA [...]
```

## 156899 - SSL/TLS Recommended Cipher Suites

### Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

### Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

### See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

### Solution

Only enable support for recommened cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

### Plugin Output

tcp/631/www

## 25240 - Samba Server Detection

### Synopsis

An SMB server is running on the remote host.

### Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

### See Also

https://www.samba.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

### Plugin Output

tcp/445/cifs

```
The remote host tries to hide its SMB server type by changing the MAC
address and the LAN manager name.

However by sending several valid and invalid RPC requests it was
possible to fingerprint the remote SMB server as Samba.
```

## 104887 - Samba Version

### Synopsis

It was possible to obtain the samba version from the remote operating system.

### Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 4.3.11-Ubuntu
```

## 96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

### Synopsis

The remote Windows host supports the SMBv1 protocol.

### Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

### See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

### Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

### Risk Factor

None

### References

XREF IAVT:0001-T-0710

### Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

### Plugin Output

tcp/445/cifs

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/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.
```

## 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/631/www

```
A TLSv1 server answered on this port.
```

tcp/631/www

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

## 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/3306/mysql

```
A MySQL 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/3500/www

```
A web server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/8080/www

```
A web server is running on this port.
```

## 17975 - Service Detection (GET request)

### Synopsis

The remote service could be identified.

### Description

It was possible 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

### References

XREF IAVT:0001-T-0935

### Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

### Plugin Output

tcp/6697/irc

```
An IRC daemon is listening on this port.
```

## 22869 - Software Enumeration (SSH)

### Synopsis

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

### Description

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

### Solution

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

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0502 |

### Plugin Information

Published: 2006/10/15, Modified: 2022/09/06

### Plugin Output

tcp/0

## 121010 - TLS Version 1.1 Protocol Detection

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

### See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

### Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

### Risk Factor

None

### References

XREF CWE:327

### Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

### Plugin Output

tcp/631/www

## 110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0502 |

### Plugin Information

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

### Plugin Output

tcp/22/ssh

## 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

## 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

## 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

## 192709 - Tukaani XZ Utils Installed (Linux / Unix)

### Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

### Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/03/29, Modified: 2024/06/21

### Plugin Output

tcp/0

## 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

## 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

## 186361 - VMWare Tools or Open VM Tools Installed (Linux)

### Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

### Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

### See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?c0628155

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/11/28, Modified: 2024/06/21

### Plugin Output

tcp/0

## 189731 - Vim Installed (Linux)

### Synopsis

Vim is installed on the remote Linux host.

### Description

Vim is installed on the remote Linux host.

### See Also

https://www.vim.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/01/29, Modified: 2024/06/21

### Plugin Output

tcp/0

## 135860 - WMI Not Available

### Synopsis

WMI queries could not be made against the remote host.

### Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

### See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/04/21, Modified: 2024/06/12

### Plugin Output

tcp/445/cifs

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

| | |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/80/www

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

| | |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/631/www

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

| | |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/3500/www

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

| | |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/8080/www

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/80/www

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/631/www

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/3500/www

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/8080/www

## 40773 - Web Application Potentially Sensitive CGI Parameter Detection

### Synopsis

An application was found that may use CGI parameters to control sensitive information.

### Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

### Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

### Risk Factor

None

### Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /payroll_app.php :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
user : Potential horizontal privilege escalation - try another user ID

Potentially sensitive parameters for CGI /drupal/ :

pass : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

## 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://10.0.2.9/
  - http://10.0.2.9/chat/
  - http://10.0.2.9/chat/index.php
  - http://10.0.2.9/chat/style.css
  - http://10.0.2.9/drupal/
  - http://10.0.2.9/drupal/misc/
  - http://10.0.2.9/drupal/misc/ajax.js
  - http://10.0.2.9/drupal/misc/arrow-asc.png
  - http://10.0.2.9/drupal/misc/arrow-desc.png
  - http://10.0.2.9/drupal/misc/authorize.js
  - http://10.0.2.9/drupal/misc/autocomplete.js
  - http://10.0.2.9/drupal/misc/batch.js
  - http://10.0.2.9/drupal/misc/collapse.js
  - http://10.0.2.9/drupal/misc/configure.png
  - http://10.0.2.9/drupal/misc/draggable.png
  - http://10.0.2.9/drupal/misc/drupal.js
  - http://10.0.2.9/drupal/misc/druplicon.png
  - http://10.0.2.9/drupal/misc/farbtastic/
  - http://10.0.2.9/drupal/misc/farbtastic/farbtastic.css
  - http://10.0.2.9/drupal/misc/farbtastic/farbtastic.js
  - http://10.0.2.9/drupal/misc/farbtastic/marker.png
  - http://10.0.2.9/drupal/misc/farbtastic/mask.png
```

```
- http://10.0.2.9/drupal/misc/farbtastic/wheel.png
- http://10.0.2.9/drupal/misc/favicon.ico
- http://10.0.2.9/drupal/misc/feed.png
- http://10.0.2.9/drupal/misc/form.js
- http://10.0.2.9/drupal/misc/forum-icons.png
- http://10.0.2.9/drupal/misc/grippie.png
- http://10.0.2.9/drupal/misc/help.png
- http://10.0.2.9/drupal/misc/jquery.ba-bbq.js
- http://10.0.2.9/drupal/misc/jquery.cookie.js
- http://10.0.2.9/drupal/misc/jquery.form.js
- http://10.0.2.9/drupal/misc/jquery.js
- http://10.0.2.9/drupal/misc/jquery.once.js
- http://10.0.2.9/drupal/misc/machine-name.js
- http://10.0.2.9/drupal/misc/menu-collapsed-rtl.png
- http://10.0.2.9/drupal/misc/menu-collapsed.png
- http://10.0.2.9/drupal/misc/menu-expanded.png
- http://10.0.2.9/drupal/misc/menu-leaf.png
- http://10.0.2.9/drupal/misc/message-16-error.png
- http://10.0.2.9/drupal/misc/message-16-help.png
- http://10.0.2.9/drupal/misc/message-16-info.png
- http://10.0.2.9/drupal/misc/message-16-ok.png
- http://10.0.2.9/drupa [...]
```

## 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/3500/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://10.0.2.9:3500/
  - http://10.0.2.9:3500//
  - http://10.0.2.9:3500/rails/info/properties
  - http://10.0.2.9:3500/rails/info/routes

Attached is a copy of the sitemap file.
```

## 20108 - Web Server / Application favicon.ico Vendor Fingerprinting

### Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

### Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

### Solution

Remove the 'favicon.ico' file or create a custom one for your site.

### Risk Factor

None

### Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

### Plugin Output

tcp/8080/www

## 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, /uploads, /chat, /drupal, /phpmyadmin

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
```

## 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/3500/www

```
The following directories were discovered:
//

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
```

## 10662 - Web mirroring

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2024/05/20

### Plugin Output

tcp/80/www

```
Webmirror performed 671 queries in 5s (134.0200 queries per second)

The following CGIs have been discovered :


+ CGI : /chat/index.php
  Methods : POST
  Argument : enter
   Value: Enter
  Argument : name


+ CGI : /drupal/
  Methods : GET,POST
  Argument : destination
   Value: node
  Argument : form_build_id
   Value: form-d8LdjYn0RUG0TOJvGyqs1cbfT5g2VZRXrV9DuvGs4YA
  Argument : form_id
   Value: user_login_block
  Argument : name
  Argument : op
   Value: Log in
  Argument : pass
  Argument : q
   Value: node/1
```

```
+ CGI : /payroll_app.php
  Methods : POST
  Argument : password
  Argument : s
   Value: OK
  Argument : user


+ CGI : /phpmyadmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 4334846010
  Argument : server
   Value: 1
  Argument : token
   Value: d98572319ef621d5fbbc8be5760c8ea4


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : token
   Value: d98572319ef621d5fbbc8be5760c8ea4
  Argument : url
   Value: http%3A%2F%2Fwww.phpmyadmin.net%2F


+ CGI : /phpmyadmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
   Value: zh_TW
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: d98572319ef621d5fbbc8be5760c8ea4

Directory index found at /
Directory index found at /uploads/
Directory index found at /uploads/Uw3xGVES.htm/
Directory index found at /uploads/lM3AgSkp.htm/
Directory index found at /uploads/qia4cRbL.htm/
Directory index found at /uploads/zLvUAEZ1.htm/
Directory index found at /drupal/misc/
Directory index found at /phpmyadmin/themes/pmahomme/jquery/
Directory index found at /phpmyadmin/themes/pmahomme/
Directory index found at /phpmyadmin/themes/
Directory index found at /drupal/misc/farbtastic/
Directory index found at /drupal/misc/ui/
Directory index found at /phpmyadmin/themes/pmahomme/jquery/images/
Directory index found at /phpmyadmin/themes/pmahomme/css/
Directory index found at /phpmyadmin/themes/pmahomme/img/
Directory index fou [...]
```

## 24004 - WebDAV Directory Enumeration

### Synopsis

Several directories on the remote host are DAV-enabled.

### Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

### Solution

Disable DAV support if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 2007/01/11, Modified: 2011/03/14

### Plugin Output

tcp/80/www

```
The following directories are DAV enabled :
 - /uploads/
```

## 10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

### Synopsis

It was possible to obtain the network name of the remote host.

### Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

### Plugin Output

tcp/445/cifs

```
The following 2 NetBIOS names have been gathered :

 METASPLOITABLE3-UB1404 = Computer name
 METASPLOITABLE3-UB1404 = Workgroup / Domain name
```

## 182848 - libcurl Installed (Linux / Unix)

### Synopsis

libcurl is installed on the remote Linux / Unix host.

### Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

### See Also

https://curl.se/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/10/10, Modified: 2024/06/21

### Plugin Output

tcp/0

## 17219 - phpMyAdmin Detection

### Synopsis

The remote web server hosts a database management application written in PHP.

### Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

### See Also

https://www.phpmyadmin.net/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

### Plugin Output

tcp/80/www