basic-scan

Report generated by Nessus™ Wed, 03 Apr 2024 17:29:12 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.100.86....4

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

- Suggested Remediations....223

Vulnerabilities by Host

192.168.100.86

10	14	18	6	93
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Apr 3 16:35:06 2024

End time: Wed Apr 3 17:29:11 2024

Host Information

Netbios Name:	METASPLOITABLE3-UB1404
IP:	192.168.100.86
MAC Address:	08:00:27:42:51:79
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

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://192.168.100.86/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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.38
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.39
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.40
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.41
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.42
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.43
```

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: 2024/03/22

Plugin Output

tcp/80/www

```
  Source              : X-Powered-By: PHP/5.4.5
  Installed version   : 5.4.5
```

```
    End of support date : 2015/09/03
    Announcement        : http://php.net/supported-versions.php
    Supported versions  : 8.0.x / 8.1.x
```

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

```
Nessus received a 350 response from sending the following unauthenticated request :

SITE CPFR /etc/passwd
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
URL               : http://192.168.100.86/phpmyadmin
Installed version : 3.5.8
Fixed version     : 4.8.6
```

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.

Note that this script is experimental and may be prone to false positives.

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: 2022/10/28

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=78e61cb5e7dee25a153aec44aa277899&no
cache=4334846010&server=1&js_frame=rightzz78e61cb5e7dee25a153aec44aa2778
99&nocache=4334846010&server=1&js_frame=rightyy

-------- output --------
.syntax_comment {color: #808000;}
.syntax_comment_mysql {}
.syntax_comment_ansi {}
-------- vs --------
/***********************************************************************
*******/
/* general tags */
html {
------------------------
```

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: 192.168.100.86
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 ------------------------------
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.13
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.17
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.19
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.23
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.28
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.30
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.34
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.36
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.37
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.44
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.45
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
    URL               : http://192.168.100.86/ (5.4.5 under X-Powered-By: PHP/5.4.5)
    Installed version : 5.4.5
    Fixed version     : 7.3.24
```

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

```
The following directories are browsable :

http://192.168.100.86/
http://192.168.100.86/drupal/misc/
http://192.168.100.86/drupal/misc/farbtastic/
http://192.168.100.86/drupal/misc/ui/
http://192.168.100.86/drupal/misc/ui/images/
http://192.168.100.86/phpmyadmin/themes/
http://192.168.100.86/phpmyadmin/themes/original/
http://192.168.100.86/phpmyadmin/themes/original/css/
http://192.168.100.86/phpmyadmin/themes/original/img/
http://192.168.100.86/phpmyadmin/themes/original/img/pmd/
```

```
http://192.168.100.86/phpmyadmin/themes/original/jquery/
http://192.168.100.86/phpmyadmin/themes/original/jquery/images/
http://192.168.100.86/phpmyadmin/themes/pmahomme/
http://192.168.100.86/phpmyadmin/themes/pmahomme/css/
http://192.168.100.86/phpmyadmin/themes/pmahomme/img/
http://192.168.100.86/phpmyadmin/themes/pmahomme/img/pmd/
http://192.168.100.86/phpmyadmin/themes/pmahomme/jquery/
http://192.168.100.86/phpmyadmin/themes/pmahomme/jquery/images/
http://192.168.100.86/uploads/
```

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>
]

-------- output --------


<center><h2>Welcome, <.script>alert(219);</script.></h2><br><table style
='border-radius: 25px; border: 2px solid black;' cellspacing=30><tr><th>
Username</th><th>First Name</th><th>Last Name</th><th>Salary</th></tr></
table></center>
------------------------
```

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

4.9

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

```
IP forwarding appears to be enabled on the remote host.

 Detected local MAC Address        : 080027209e43
 Response from local MAC Address   : 080027209e43

 Detected Gateway MAC Address      : 080027425179
 Response from Gateway MAC Address : 080027425179
```

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

2.2

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.12
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.16
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.24
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.26
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.27
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.29
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.32
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : X-Powered-By: PHP/5.4.5
Installed version : 5.4.5
Fixed version     : 5.4.35
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  URL               : http://192.168.100.86/ (5.4.5 under X-Powered-By: PHP/5.4.5)
  Installed version : 5.4.5
  Fixed version     : 7.3.28
```

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

```

Nessus was able to verify the issue using the following URL :

  http://192.168.100.86/phpmyadmin/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

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

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following CBC Client to Server algorithm               : cast128-cbc
Supports following CBC Client to Server algorithm               : aes192-cbc
Supports following CBC Client to Server algorithm               : aes256-cbc
Supports following CBC Client to Server algorithm               : rijndael-cbc@lysator.liu.se
Supports following CBC Client to Server algorithm               : blowfish-cbc
Supports following CBC Client to Server algorithm               : 3des-cbc
Supports following CBC Client to Server algorithm               : aes128-cbc
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-ripemd160-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following CBC Server to Client algorithm               : cast128-cbc
Supports following CBC Server to Client algorithm               : aes192-cbc
Supports following CBC Server to Client algorithm               : aes256-cbc
Supports following CBC Server to Client algorithm               : rijndael-cbc@lysator.liu.se
Supports following CBC Server to Client algorithm               : blowfish-cbc
Supports following CBC Server to Client algorithm               : 3des-cbc
Supports following CBC Server to Client algorithm               : aes128-c [...]
```

90317 - SSH Weak Algorithms Supported

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  arcfour
  arcfour128
  arcfour256

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

  arcfour
  arcfour128
  arcfour256
```

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=swlnkl HTTP/1.1
Host: 192.168.100.86
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=swlnkl HTTP/1.1
Host: 192.168.100.86
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: 192.168.100.86
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: 144
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-7Qs8m0NAhooxfzQv28l44KUnR_Szibb3_cFJANf2ZE4&q= [...]
```

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

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.100.86/chat/
  - http://192.168.100.86/chat/index.php
  - http://192.168.100.86/drupal/
  - http://192.168.100.86/payroll_app.php
  - http://192.168.100.86/phpmyadmin/
  - http://192.168.100.86/phpmyadmin/index.php
  - http://192.168.100.86/phpmyadmin/url.php
```

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: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.4.5
  Installed version : 5.4.5
  Fixed version     : 5.4.31
```

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

```

The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```

The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```

The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

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

```
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
```

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)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
  URL        : http://192.168.100.86/
  Version    : 2.4.99
  Source     : Server: Apache/2.4.7 (Ubuntu)
  backported : 1
  os         : ConvertedUbuntu
```

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

```
Give Nessus credentials to perform local checks.
```

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

```
Give Nessus credentials to perform local checks.
```

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

```
Give Nessus credentials to perform local checks.
```

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=swlnkl

-------- output --------
<script src="./js/functions.js?ts=1365422810" type="text/javascrip [...]
<script src="./js/jquery/jquery.qtip-1.0.0-rc3.js?ts=1365422810" t [...]
<script src="./js/messages.php?lang=en&amp;db=swlnkl&amp;collation_conne
ction=utf8_general_ci&amp;token=c832fe4817f0033390dd48286597e48a" type="
text/javascript"></script>
<script src="./js/get_image.js.php?theme=pmahomme" type="text/java [...]
<script type="text/javascript">
------------------------
```

```
+ The 'lang' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?lang=swlnkl

-------- output --------
</form>

<div><div class="error">Unknown language: swlnkl.</div><div class="notic
e">Cookies must be enabled past this point.</div></div></div>
</body>
</html>
------------------------

+ The 'table' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?table=swlnkl

-------- output --------

<form method="post" action="index.php" target="_parent">
<input type="hidden" name="db" value="" /><input type="hidden" name="tab
le" value="swlnkl" /><input type="hidden" name="lang" value="en" /><inpu
t type="hidden" name="collation_connection" value="utf8_general_ci" /><i
nput type="hidden" name="token" value="8ac27628328782e80524d35d83281a1d"
 /><fieldset><legend xml:lang="en" dir="ltr">Language</legend>
<select name="lang" class="autosubmit" xml:lang="en" dir="ltr">
<option value="ar">&#1575;&#1604;&#1593;&#1585;&#1576;&#1610;&#157 [...]
------------------------

+ The 'pma_username' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?pma_username=swlnkl

-------- output --------
<div class="item">
<label for="input_username">Username:</label>
<input type="text" name="pma_username" id="input_username" value="swlnkl
" size="24" class="textfield"/>
</div>
<div class="item">
------------------------

+ The [...]
```

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
- uncontrolled redirection
- local file inclusion
- arbitrary command execution
- directory traversal (extended test)
- 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
```

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: 2024/03/19

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:drupal:drupal:7.5 -> Drupal
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:6.6.1p1 -> OpenBSD OpenSSH
  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
```

132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2024-04-03 14:39:51
Port: 22
```

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 : 95
```

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

```
URL     : http://192.168.100.86/drupal
Version : 7.5
```

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 :

08:00:27:42:51:79 : 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

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:42:51:79
```

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) [192.168.100.86]
```

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/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/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: Wed, 03 Apr 2024 14:43:11 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Vary: Accept-Encoding
  Content-Length: 1953
  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/unknown.gif" alt="[   ]"></td><td><a
 href="CTHgwFG.php">CTHgwFG.php</a></td><td align="right">2024-04-03 00:02  </td><td align="right">
 81 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a
 href="DubLF.php">DubLF.php</a></td><td align="right">2024-04-02 23:57  </td><td align="right"> 82
 </td><td>&nbsp;</td></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>&nbsp;</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>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a
 href="fninu.php">fninu.php</a></td><td align="right">2024-04-02 23:55  </td><td align="right"> 80
 </td><td>&nbsp;</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>&nbsp;</td></tr>
<tr><td val [...]
```

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: b99eeaf8-9416-43cd-b6fc-1b17ea1e738d
  X-Runtime: 0.001673
  Server: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
  Date: Wed, 03 Apr 2024 14:43:11 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(data:image/
  png;base64,iVBORw0KGgoAAAANSUhEUgAAADIAAABACAYAAABY1SR7AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAGZhJREF
  t5Sr9aurl6qO0l3Z9/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: Wed, 03 Apr 2024 14:43:11 GMT
  Content-Type: text/html
  Content-Length: 795
  Connection: close
  Server: Jetty(8.1.7.v20120910)

Response Body :
```

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

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -1 seconds.
```

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-1-5-21-2365808667-1472566119-3200918539

The value of 'RestrictAnonymous' setting is : unknown
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu
The remote SMB Domain Name is : METASPLOITABLE3-UB1404
```

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

```
Here are the SMB shares available on the remote host :

  - print$
  - public
  - IPC$
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.100.86/
  - http://192.168.100.86/CTHgwFG.php
  - http://192.168.100.86/DubLF.php
  - http://192.168.100.86/chat/
  - http://192.168.100.86/chat/index.php
  - http://192.168.100.86/drupal/
  - http://192.168.100.86/drupal/misc/
  - http://192.168.100.86/drupal/misc/farbtastic/
  - http://192.168.100.86/drupal/misc/ui/
  - http://192.168.100.86/drupal/misc/ui/images/
  - http://192.168.100.86/fninu.php
```

```
    - http://192.168.100.86/payroll_app.php
    - http://192.168.100.86/phpmyadmin/
    - http://192.168.100.86/phpmyadmin/index.php
    - http://192.168.100.86/phpmyadmin/themes/
    - http://192.168.100.86/phpmyadmin/themes/original/
    - http://192.168.100.86/phpmyadmin/themes/original/css/
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_left.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_print.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_right.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/img/
    - http://192.168.100.86/phpmyadmin/themes/original/img/pmd/
    - http://192.168.100.86/phpmyadmin/themes/original/info.inc.php
    - http://192.168.100.86/phpmyadmin/themes/original/jquery/
    - http://192.168.100.86/phpmyadmin/themes/original/jquery/images/
    - http://192.168.100.86/phpmyadmin/themes/original/layout.inc.php
    - http://192.168.100.86/phpmyadmin/themes/original/sprites.lib.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_left.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_print.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_right.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/img/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/img/pmd/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/info.inc.php
    - http://1 [...]
```

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

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.100.86:3500/
  - http://192.168.100.86:3500//
  - http://192.168.100.86:3500/rails/info/properties
  - http://192.168.100.86:3500/rails/info/routes
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.100.86/
  - http://192.168.100.86/CTHgwFG.php
  - http://192.168.100.86/DubLF.php
  - http://192.168.100.86/chat/
  - http://192.168.100.86/chat/index.php
  - http://192.168.100.86/drupal/
  - http://192.168.100.86/drupal/misc/
  - http://192.168.100.86/drupal/misc/farbtastic/
  - http://192.168.100.86/drupal/misc/ui/
  - http://192.168.100.86/drupal/misc/ui/images/
  - http://192.168.100.86/fninu.php
  - http://192.168.100.86/payroll_app.php
  - http://192.168.100.86/phpmyadmin/
  - http://192.168.100.86/phpmyadmin/index.php
  - http://192.168.100.86/phpmyadmin/themes/
  - http://192.168.100.86/phpmyadmin/themes/original/
```

```
    - http://192.168.100.86/phpmyadmin/themes/original/css/
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_left.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_print.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/css/theme_right.css.php
    - http://192.168.100.86/phpmyadmin/themes/original/img/
    - http://192.168.100.86/phpmyadmin/themes/original/img/pmd/
    - http://192.168.100.86/phpmyadmin/themes/original/info.inc.php
    - http://192.168.100.86/phpmyadmin/themes/original/jquery/
    - http://192.168.100.86/phpmyadmin/themes/original/jquery/images/
    - http://192.168.100.86/phpmyadmin/themes/original/layout.inc.php
    - http://192.168.100.86/phpmyadmin/themes/original/sprites.lib.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_left.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_print.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/css/theme_right.css.php
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/img/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/img/pmd/
    - http://192.168.100.86/phpmyadmin/themes/pmahomme/info.inc.php
    - http://192.168.100.86/phpmyadmin [...]
```

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.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/631

```
Port 631/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/3500/www

```
Port 3500/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/6697/irc

```
Port 6697/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

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: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.2
Nessus build : 20029
Plugin feed version : 202404031140
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : basic-scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.87
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 164.711 ms
Thorough tests : yes
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : 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 : 2024/4/3 16:35 CEST
Scan duration : 3229 sec
Scan for malware : no
```

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: 2023/11/08

Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

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: 2024/03/27

Plugin Output

tcp/22/ssh

```
  Service : ssh
  Version : 6.6.1p1
  Banner  : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
```

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: 2022/10/12

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.4.5
  Source  : X-Powered-By: PHP/5.4.5
```

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: 2024/03/19

Plugin Output

tcp/0

```


. You need to take the following 4 actions :


[ PHP 5.4.x < 5.4.45 Multiple Vulnerabilities (85885) ]

+ Action to take : Upgrade to PHP version 5.4.45 or later.

+Impact : Taking this action will resolve 95 different vulnerabilities (CVEs).



[ ProFTPD mod_copy Information Disclosure (84215) ]

+ Action to take : Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.


[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or
 disable the affected algorithms.


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

+ Action to take : Upgrade to phpMyAdmin version 4.8.6 or later.
```

```
Alternatively, apply the patches referenced in the vendor advisories.
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 08:00:27:42:51:79
```

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.
```

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 [...]
```

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
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

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

  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com

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

  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 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
```

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

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/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/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.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

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

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.100.87 to 192.168.100.86 :
192.168.100.87
192.168.100.86

Hop Count: 1
```

66293 - Unix Operating System on Extended Support

Synopsis

The remote host is running an operating system that is on extended support.

Description

According to its version, the remote host uses a Unix or Unix-like operating system that has transitioned to an extended portion in its support life cycle. Continued access to new security updates requires payment of an additional fee and / or configuration changes to the package management tool. Without that, the host likely will be missing security updates.

Solution

Ensure that the host subscribes to the vendor's extended support plan and continues to receive security updates.

Risk Factor

None

References

XREF	IAVA:0001-A-0648

Plugin Information

Published: 2013/05/02, Modified: 2023/05/10

Plugin Output

tcp/0

```
Ubuntu 14.04 support ends on 2019-04-30 (end of maintenance) / 2024-04-30 (end of extended security
 maintenance).
```

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: 2024/03/26

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

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

```

The following cookie does not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :

```

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

```

The following cookie does not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :

```

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

```
The following cookie does not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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

```
The following cookies do not set the secure cookie flag :

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_mcrypt_iv
Path : /phpmyadmin/
Value : 8vro603A%2BhA%3D
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_collation_connection
Path : /phpmyadmin/
Value : utf8_general_ci
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : b03befcd3f9636d5279f066ad138e20a1d24a5e7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

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

```
The following cookies do not set the secure cookie flag :

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_mcrypt_iv
Path : /phpmyadmin/
Value : 8vro603A%2BhA%3D
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_collation_connection
Path : /phpmyadmin/
Value : utf8_general_ci
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : b03befcd3f9636d5279f066ad138e20a1d24a5e7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

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

```
The following cookies do not set the secure cookie flag :

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_mcrypt_iv
Path : /phpmyadmin/
Value : 8vro603A%2BhA%3D
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_collation_connection
Path : /phpmyadmin/
Value : utf8_general_ci
Domain :
Version : 1
Expires : Fri, 03-May-2024 14:42:06 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : 5aadcb9b1f77e9557d9a27bf1b1cc85e
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : b03befcd3f9636d5279f066ad138e20a1d24a5e7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

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://192.168.100.86/
  - http://192.168.100.86/CTHgwFG.php
  - http://192.168.100.86/DubLF.php
  - http://192.168.100.86/chat/
  - http://192.168.100.86/chat/index.php
  - http://192.168.100.86/chat/style.css
  - http://192.168.100.86/drupal/
  - http://192.168.100.86/drupal/misc/
  - http://192.168.100.86/drupal/misc/ajax.js
  - http://192.168.100.86/drupal/misc/arrow-asc.png
  - http://192.168.100.86/drupal/misc/arrow-desc.png
  - http://192.168.100.86/drupal/misc/authorize.js
  - http://192.168.100.86/drupal/misc/autocomplete.js
  - http://192.168.100.86/drupal/misc/batch.js
  - http://192.168.100.86/drupal/misc/collapse.js
  - http://192.168.100.86/drupal/misc/configure.png
  - http://192.168.100.86/drupal/misc/draggable.png
  - http://192.168.100.86/drupal/misc/drupal.js
  - http://192.168.100.86/drupal/misc/druplicon.png
  - http://192.168.100.86/drupal/misc/farbtastic/
  - http://192.168.100.86/drupal/misc/farbtastic/farbtastic.css
  - http://192.168.100.86/drupal/misc/farbtastic/farbtastic.js
```

```
    - http://192.168.100.86/drupal/misc/farbtastic/marker.png
    - http://192.168.100.86/drupal/misc/farbtastic/mask.png
    - http://192.168.100.86/drupal/misc/farbtastic/wheel.png
    - http://192.168.100.86/drupal/misc/favicon.ico
    - http://192.168.100.86/drupal/misc/feed.png
    - http://192.168.100.86/drupal/misc/form.js
    - http://192.168.100.86/drupal/misc/forum-icons.png
    - http://192.168.100.86/drupal/misc/grippie.png
    - http://192.168.100.86/drupal/misc/help.png
    - http://192.168.100.86/drupal/misc/jquery.ba-bbq.js
    - http://192.168.100.86/drupal/misc/jquery.cookie.js
    - http://192.168.100.86/drupal/misc/jquery.form.js
    - http://192.168.100.86/drupal/misc/jquery.js
    - http://192.168.100.86/drupal/misc/jquery.once.js
    - http://192.168.100.86/drupal/misc/machine-name.js
    - http://192.168.100.86/drupal/misc/menu-collapsed-rtl.png
    - http://192.168.100.86/drupal/misc/menu-collapsed.png
    - http://192.168.100.86/drupal [...]
```

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://192.168.100.86:3500/
  - http://192.168.100.86:3500//
  - http://192.168.100.86:3500/rails/info/properties
  - http://192.168.100.86:3500/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

```
  MD5 fingerprint : ed7d5c39c69262f4ba95418d4f909b10
  Web server      : jetty 5.1.14
```

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: 2021/08/17

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: 2021/08/17

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: 2024/03/19

Plugin Output

tcp/80/www

```
Webmirror performed 666 queries in 3s (222.000 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-7Qs8m0NAhooxfzQv28l44KUnR_Szibb3_cFJANf2ZE4
  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: 25bb830d6e2a82c470188e230632095c


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : token
   Value: 25bb830d6e2a82c470188e230632095c
  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: 25bb830d6e2a82c470188e230632095c

Directory index found at /
Directory index found at /uploads/
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 found at /phpmyadmin/themes/original/
Directory index found at /drupal/misc/ui/images/
Directory index found at /phpmyadmin/themes/pmahomme/img/pmd/
Directory index found at /phpmyadmin/themes/ori [...]
```

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
```

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

```

The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.5.8
  URL     : http://192.168.100.86/phpmyadmin/
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 91% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
PHP 5.4.x < 5.4.45 Multiple Vulnerabilities: Upgrade to PHP version 5.4.45 or later.	95	1
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795): Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.	1	1
phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.	1	1
ProFTPD mod_copy Information Disclosure: Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.	0	1