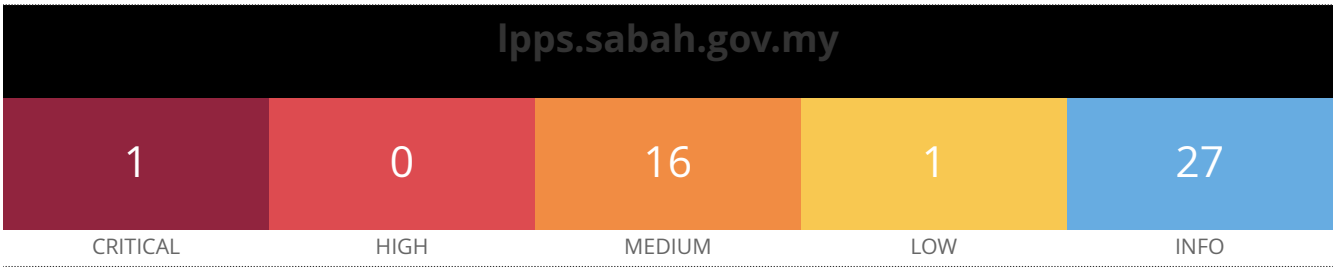
Sabah Government Website Assessment 1st of Month

Sabah-Net Nessus Report

Report generated by Nessus™ Mon, 01 Aug 2022 05:09:30 +08

Vulnerabilities by Host

Vulnerabilities by Host



Scan Information

Start time: Mon Aug 1 02:28:44 2022
End time: Mon Aug 1 03:29:48 2022

Host Information

DNS Name: lpps.sabah.gov.my
IP: 27.0.4.70
OS: Linux Kernel 2.6

Vulnerabilities

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

Plugin Information

Published: 2012/05/04, Modified: 2022/07/26

Plugin Output

tcp/443/www

```
Source              : X-Powered-By: PHP/7.3.13
Installed version   : 7.3.13
End of support date : 2021/12/06
Announcement        : http://php.net/supported-versions.php
Supported versions  : 7.4.x / 8.0.x / 8.1.x
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

https://security.paloaltonetworks.com/PAN-SA-2020-0007

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/05/28, Modified: 2021/09/09

Plugin Output

tcp/443/www

```
URL               : https://lpps.sabah.gov.my/core/assets/vendor/jquery/jquery.min.js?v=3.4.1
Installed version : 3.4.1
Fixed version     : 3.5.0
```

141355 - PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Mulitiple 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 7.2.x prior to 7.2.34, 7.3.x prior to 7.3.23 or 7.4.x prior to 7.4.11. It is, therefore, affected by multiple vulnerabilties:

- A weak cryptography vulnerability exists in PHP's openssl_encrypt function due to a failure to utilize all provided IV bytes. An unauthenticated, remote attacker could exploit this to reduce the level of security provided by the encryption scheme or affect the integrity of the encrypted data (CVE-2020-7069).

- A cookie forgery vulnerability exists in PHP's HTTP processing functionality. An unauthenticated, remote could expoit this to forge HTTP cookies which were supposed to be secure. (CVE-2020-7070)

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

See Also

http://bugs.php.net/79601

http://bugs.php.net/79699

https://www.php.net/ChangeLog-7.php#7.2.34

https://www.php.net/ChangeLog-7.php#7.3.23

https://www.php.net/ChangeLog-7.php#7.4.11

Solution

Upgrade to PHP version 7.2.34, 7.3.23, 7.4.11 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/10/09, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
```

```
    Fixed version     : 7.3.23
```

140532 - PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability

Synopsis

The version of PHP running on the remote web server is affected by a memory leak vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is 7.2.x or 7.3.x prior to 7.3.21. It is, therefore affected by a memory leak vulnerability in the LDAP component. An unauthenticated, remote attacker could exploit this issue to cause a denial-of-service condition.

See Also

https://www.php.net/ChangeLog-7.php#7.3.22

Solution

Upgrade to PHP version 7.3.22 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/09/11, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.22
```

134162 - PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities

Synopsis

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

Description

According to its banner, the version of PHP running on the remote web server is either 7.2.x prior to 7.2.28, 7.3.x prior to 7.3.15, or 7.4.x prior to 7.4.3. It is, therefore, affected by multiple vulnerabilities:

- A heap-based buffer overflow condition exists in phar_extract_file() function due to incorrect loop termination. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2020-7061)

- A denial of service (DoS) vulnerability exists in PHP SessionUpload Progress functions due to Null Pointer Dereference. An unauthenticated, remote attacker can exploit this issue to cause the php service to stop responding. (CVE-2020-7062)

- An Insecure File Permissions on the buildFromIterator function gives all access permission to Tar files. (CVE-2020-7063)

See Also

http://php.net/ChangeLog-7.php#7.2.28

http://php.net/ChangeLog-7.php#7.3.15

http://php.net/ChangeLog-7.php#7.4.3

Solution

Upgrade to PHP version 7.2.28, 7.3.15, 7.4.3 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/02/28, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.15
```

136741 - PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)

Synopsis

The version of PHP running on the remote web server is affected by a denial of service vulnerability

Description

According to its self-reported version number, the version of PHP running on the remote web server is 7.2.x prior to 7.2.31, 7.3.x prior to 7.3.18 or 7.4.x prior to 7.4.6. It is, therefore, affected by a denial of service (DoS) vulnerability in its HTTP file upload component due to a failure to clean up temporary files created during the file upload process. An unauthenticated, remote attacker can exploit this issue, by repeatedly submitting uploads with long file or field names, to exhaust disk space and cause a DoS condition.

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

See Also

http://www.nessus.org/u?948f4dd6

http://www.nessus.org/u?a05c7b46

http://www.nessus.org/u?504e39bf

Solution

Upgrade to PHP version 7.2.31, 7.3.18, 7.4.6 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/05/21, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.18
```

134944 - PHP 7.3.x < 7.3.16 Multiple Vulnerabilities

Synopsis

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

Description

According to its banner, the version of PHP running on the remote web server is 7.3.x prior to 7.3.16. It is, therefore, affected by the following vulnerabilities:

- An out of bounds read resulting in the use of an uninitialized value in exif (CVE-2020-7064)

- A stack buffer overflow in allows overwriting of a stack-allocated buffer with an overflown array from .rodata. (CVE-2020-7065)

- get_headers() silently truncates anything after a null byte in the URL it uses. An unauthenticated, remote attacker can exploit this to leak sensitive information or cause the web server to unexpectedly process attacker-controlled data. (CVE-2020-7066) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.php.net/ChangeLog-7.php#7.3.16

Solution

Upgrade to PHP version 7.3.16 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/03/27, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.16
```

135918 - PHP 7.3.x < 7.3.17 Out of Bounds Read Vulnerability

Synopsis

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

Description

According to its banner, the version of PHP running on the remote web server is 7.3.x prior to 7.3.17. It is, therefore, affected by an out-of-bounds read error in its url decoding component due to insufficient validation of user-supplied input. An unauthenticated, remote attacker can exploit this, by sending specially crafted requests, to cause a denial of service (DoS) condition or execution of arbitrary code.

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

See Also

https://www.php.net/ChangeLog-7.php#7.3.17

Solution

Upgrade to PHP version 7.3.17 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/04/23, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.17
```

143449 - PHP 7.3.x < 7.3.25 / 7.4.x < 7.4.13 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is 7.3.x prior to 7.3.25 or 7.4.x prior to 7.4.13. It is, therefore, affected by multiple vulnerabilities as specified by the changelogs of the respective fixed releases.

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

See Also

https://www.php.net/ChangeLog-7.php#7.3.25

https://www.php.net/ChangeLog-7.php#7.4.13

Solution

Upgrade to PHP version 7.3.25, 7.4.13 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/12/03, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL               : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.25
```

144947 - PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error

Synopsis

The version of PHP running on the remote web server is affected by an input validation error

Description

The version of PHP installed on the remote host is 7.3.x prior to 7.3.26, 7.4.x prior to 7.4.14, or 8.x prior to 8.0.1.

It is, therefore, affected by an input validation error due to insufficient validation of a URL, as specified by the changelogs of the respective fixed releases. An unauthenticated, remote attacker can exploit this, by including an '@'

character, in order to bypass the URL filter.

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

See Also

https://www.php.net/ChangeLog-7.php#7.3.26

https://www.php.net/ChangeLog-7.php#7.4.14

https://www.php.net/ChangeLog-8.php#8.0.1

Solution

Upgrade to PHP version 7.3.26, 7.4.14, 8.0.1 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/01/14, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.26
```

146311 - PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS

Synopsis

The version of PHP running on the remote web server is affected by a denial of service vulnerability.

Description

The version of PHP installed on the remote host is 7.3.x prior to 7.3.27, 7.4.x prior to 7.4.15, or 8.x prior to 8.0.2.

It is, therefore, affected by a denial of service (DoS) vulnerability due to a null dereference in SoapClient. An unauthenticated, remote attacker can exploit this, by providing an XML to the SoapCLient query() function without an existing field, in order to cause PHP to crash.

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

See Also

https://www.php.net/ChangeLog-7.php#7.3.27

https://www.php.net/ChangeLog-7.php#7.4.15

https://www.php.net/ChangeLog-8.php#8.0.2

Solution

Upgrade to PHP version 7.3.27, 7.4.15, 8.0.2 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/02/09, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.27
```

154663 - PHP 7.3.x < 7.3.32

Synopsis

The version PHP running on the remote web server is affected by a vulnerability.

Description

The version of PHP installed on the remote host is prior to 7.3.32. It is, therefore, affected by a vulnerability as referenced in the Version 7.3.32 advisory.

- In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower- privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.

(CVE-2021-21703)

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://bugs.php.net/81026

http://php.net/ChangeLog-7.php#7.3.32

Solution

Upgrade to PHP version 7.3.32 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/10/28, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.32
```

155590 - PHP 7.3.x < 7.3.33

Synopsis

The version PHP running on the remote web server is affected by a vulnerability.

Description

The version of PHP installed on the remote host is prior to 7.3.33. It is, therefore, affected by a vulnerability as referenced in the Version 7.3.33 advisory.

- In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended. (CVE-2021-21707)

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://bugs.php.net/79971

http://php.net/ChangeLog-7.php#7.3.33

Solution

Upgrade to PHP version 7.3.33 or later.

Risk Factor

Medium

Plugin Information

Published: 2021/11/18, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.33
```

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

Plugin Information

Published: 2020/11/06, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL               : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.24
```

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

Plugin Information

Published: 2021/08/26, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL              : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.28
```

134220 - nginx < 1.17.7 Information Disclosure

Synopsis

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

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/03/05, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL               : http://lpps.sabah.gov.my/
Installed version : 1.15.12
Fixed version     : 1.17.7
```

134220 - nginx < 1.17.7 Information Disclosure

Synopsis

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

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

Risk Factor

Medium

Plugin Information

Published: 2020/03/05, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL               : https://lpps.sabah.gov.my/
Installed version : 1.15.12
Fixed version     : 1.17.7
```

139569 - PHP 7.3.x < 7.3.21 Use-After-Free Vulnerability

Synopsis

The version of PHP running on the remote web server is affected by a use-after-free vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is 7.3.x prior to 7.3.21. It is, therefore affected by a use-after-free vulnerability in the phar_parse function due to mishandling of the actual_alias variable. An unauthenticated, remote attacker could exploit this issue by dereferencing a freed pointer which could lead to arbitrary code execution.

See Also

https://bugs.php.net/bug.php?id=79797

https://www.php.net/ChangeLog-7.php#7.3.21

Solution

Upgrade to PHP version 7.3.21

Risk Factor

Low

Plugin Information

Published: 2020/08/13, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL               : https://lpps.sabah.gov.my/ (7.3.13 under X-Powered-By: PHP/7.3.13)
Installed version : 7.3.13
Fixed version     : 7.3.21
```

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

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/443/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'field_file_category_target_id' parameter of the /downloads CGI :

/downloads?field_file_category_target_id=%00qqimcq

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


[...] _file_category_target_id":"\u0000qqimcq"}},"pluralDelimiter":"\u0003","s [...]
<script src="/core/assets/vendor/jquery/jquery.min.js?v=3.4.1"></script>
<script src="/core/assets/vendor/underscore/underscore-min.js?v=1. [...]
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

https://lpps.sabah.gov.my/downloads?field_file_category_target_id=%00qqimcq
```

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/443/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]

cross-site scripting (comprehensive test): S=8          SP=8         AP=12        SC=0         AC=12

persistent XSS                           : S=8          SP=8         AP=12        SC=0         AC=12

arbitrary command execution              : S=32         SP=32        AP=48        SC=0         AC=48

web code injection                       : S=2          SP=2         AP=3         SC=0         AC=3

script injection                         : S=1          SP=1         AP=1         SC=1         AC=1

HTML injection                           : S=5          SP=5         AP=5         SC=5         AC=5

arbitrary command execution (time based) : S=12         SP=12        AP=18        SC=0         AC=18

XML injection                            : S=2          SP=2         AP=3         SC=0         AC=3

unseen parameters                        : S=70         SP=70        AP=105       SC=0
 AC=105
```

```
directory traversal (write access)       : S=4          SP=4          AP=6          SC=0          AC=6

SQL injection (2nd order)                : S=2          SP=2          AP=3          SC=0          AC=3

on site request forgery                  : S=1          SP=1          AP=1          SC=1          AC=1

blind SQL injection (4 requests)         : S=8          SP=8          AP=12         SC=0          AC=12

HTTP response splitting                  : S=9          SP=9          AP=9          SC=9          AC=9

directory traversal (extended test)      : S=102        SP=102        AP=153        SC=0
 AC=153
header injection                         : S=2          SP=2          AP=2          SC=2          AC=2

injectable parameter                     : S=4          SP=4          AP=6          SC=0          AC=6

local file inclusion                   [...]
```

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/443/www

```
The following tests timed out without finding any flaw :
- SQL injection
```

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

Plugin Information

Published: 2005/07/07, Modified: 2022/07/05

Plugin Output

tcp/443/www

```
URL     : https://lpps.sabah.gov.my/
Version : 8.8.1
```

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/443/www

```
27 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://appjpan.sabah.gov.my/ekompetensi/ - /intranet
http://lpps.com.my/webmail              - /
http://railway.sabah.gov.my             - /
http://sisharta.jpkn.sabah.gov.my/      - /intranet
http://sww.jpkn.sabah.gov.my/Outstation/default.asp - /intranet
http://sww.jpkn.sabah.gov.my/eKursus/mainpage.asp - /intranet
http://sww.jpkn.sabah.gov.my/eleave/    - /intranet
http://sww.jpkn.sabah.gov.my/epergerakan/ - /intranet
http://sww.jpkn.sabah.gov.my/izinKeluarNegeri/default.asp - /intranet
http://sww.jpkn.sabah.gov.my/izinhadirseminar/default.htm - /intranet
http://sww.jpkn.sabah.gov.my/jabatancetakkerajaan/ - /intranet
http://sww.jpkn.sabah.gov.my/prestasi/  - /intranet
http://sww.jpkn.sabah.gov.my/semakanbayaran/ - /intranet
http://sww.jpkn.sabah.gov.my/smapan/frontpage.htm - /intranet
http://sww.jpkn.sabah.gov.my/smapan/personalrec.asp - /intranet
http://www.jkr.sabah.gov.my/            - /
http://www.met.gov.my/                  - /intranet
http://www.sabah.gov.my                 - /govlinks
http://www.spins.sabah.gov.my/          - /intranet
http://www.spsb.com.my                  - /
https://cdn.jsdelivr.net/bootstrap/3.3.7/css/bootstrap.css - /
https://egjpkn.sabah.gov.my             - /intranet
https://i-adu.sabah.gov.my/aduan-uins/login - /intranet
https://kkrs.sabah.gov.my/en/           - /govlinks
https://www.facebook.com/lpps.com.my/   - /
```

```
https://www.google.com/maps/embed?pb=!1m14!1m8!1m3!1d3968.0166850624114!2d116.0798099!3d5.9924382!
3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x323b6a2bf868a63d%3A0xa3d8cd38cb312547!2sSabah+Ports+Authority!
5e0!3m2!1sen!2smy!4v1539739169404 - /
https://www.sabah.gov.my/ecircular/default.aspx - /intranet
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

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 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 UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  POST GET are allowed on :

    /
    /Admin
    /News
    /admin
    /batch
    /downloads
    /intranet

  - HTTP methods GET HEAD HEAD HEAD OPTIONS POST are allowed on :

    /core
    /sites


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 :

    /
    /Admin
    /News
    /admin
    /batch
    /core
    /downloads
    /intranet
    /sites

  - Invalid/unknown HTTP methods are allowed on :

    /
    /Admin
    /News
    /admin
    /batch
    /core
    /downloads
    /intranet
    /sites
```

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

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

nginx/1.15.12
```

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

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :

nginx/1.15.12
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx/1.15.12
  Date: Sun, 31 Jul 2022 18:54:41 GMT
  Content-Type: text/html
  Content-Length: 170
  Connection: keep-alive
  Location: https://lpps.sabah.gov.my/

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.15.12</center>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx/1.15.12
  Date: Sun, 31 Jul 2022 18:54:41 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  X-Powered-By: PHP/7.3.13
  Cache-Control: must-revalidate, no-cache, private
  X-Drupal-Dynamic-Cache: MISS
  X-UA-Compatible: IE=edge
  Content-language: en
  X-Content-Type-Options: nosniff
  X-Frame-Options: SAMEORIGIN
  expires: -1
  Vary: Accept-Encoding
  X-Generator: Drupal 8 (https://www.drupal.org)
  X-Drupal-Cache: HIT
  pragma: no-cache

Response Body :
```

```
<!DOCTYPE html>
<html  lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://
purl.org/dc/terms/  foaf: http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://
www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/  sioc: http://rdfs.org/sioc/ns#
 sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd: http://
www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<noscript><style>form.antibot * :not(.antibot-message) { display: none !important; }</style>
</noscript><meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Home | Lembaga Pelabuhan-Pelabuhan Sabah</title>
    <link rel="stylesheet" media="all" href="/core/modules/system/css/components/align.module.css?
r1pvz6" />
<link rel="stylesheet" media="all" href="/core/modules/system/css/components/fieldgroup.module.css?
r1pvz6" />
<link rel="stylesheet" media="all" href="/core/modules/system/css/components/container-
inline.module.css?r1pvz6" />
<link rel="stylesheet" media="all" href="/core/modules/system/css/components/clearfix.module.css?
r1pvz6" />
<link rel="stylesheet" media="all" href="/core/modules/system/css/components/detai [...]
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
  Request         : http://lpps.sabah.gov.my/
  HTTP response   : HTTP/1.1 301 Moved Permanently
  Redirect to     : https://lpps.sabah.gov.my/
  Redirect type   : 30x redirect


Note that Nessus did not receive a 200 OK response from the
last examined redirect.
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2020/01/23

Plugin Output

tcp/443/www

```
URL     : https://lpps.sabah.gov.my/core/assets/vendor/jquery/jquery.min.js?v=3.4.1
Version : 3.4.1
```

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/443/www

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

  - https://lpps.sabah.gov.my/
  - https://lpps.sabah.gov.my/News
  - https://lpps.sabah.gov.my/announcement-archive
  - https://lpps.sabah.gov.my/career
  - https://lpps.sabah.gov.my/downloads
  - https://lpps.sabah.gov.my/events
  - https://lpps.sabah.gov.my/govlinks
  - https://lpps.sabah.gov.my/intranet
  - https://lpps.sabah.gov.my/news
  - https://lpps.sabah.gov.my/photo-gallery
```

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: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.2.0
Nessus build : 20075
Plugin feed version : 202207310544
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1110-x86-64
Scan type : Normal
Scan name : Sabah Government Website Assessment 1st of Month
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.250.4.105
Port scanner(s) : nessus_tcp_scanner
Port range : 80,443
Ping RTT : 47.658 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 1 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 600
Max checks : 600
Recv timeout : 30
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2022/8/1 2:28 +08
Scan duration : 3661 sec
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/80/www

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

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/07/19

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

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

Plugin Information

Published: 2010/08/04, Modified: 2022/04/15

Plugin Output

tcp/443/www

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

  Version : 7.3.13
  Source  : X-Powered-By: PHP/7.3.13
```

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: 2022/07/19

Plugin Output

tcp/0

```
. You need to take the following 2 actions :

[ PHP 7.3.x < 7.3.33 (155590) ]

+ Action to take : Upgrade to PHP version 7.3.33 or later.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).


[ nginx < 1.17.7 Information Disclosure (134220) ]

+ Action to take : Upgrade to nginx version 1.17.7 or later.
```

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/443/www

```
The following sitemap was created from crawling linkable content on the target host :

  - https://lpps.sabah.gov.my/
  - https://lpps.sabah.gov.my/News
  - https://lpps.sabah.gov.my/announcement-archive
  - https://lpps.sabah.gov.my/career
  - https://lpps.sabah.gov.my/downloads
  - https://lpps.sabah.gov.my/events
  - https://lpps.sabah.gov.my/govlinks
  - https://lpps.sabah.gov.my/intranet
  - https://lpps.sabah.gov.my/news
  - https://lpps.sabah.gov.my/photo-gallery

Attached is a copy of the sitemap file.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

tcp/443/www

```
The following directories were discovered:
/Admin, /News, /admin, /downloads, /intranet, /sites, /batch, /core

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
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://lpps.sabah.gov.my/CAwdOshawDk1.html
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :

#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
# CSS, JS, Images
Allow: /core/*.css$
```

```
Allow: /core/*.css?
Allow: /core/*.js$
Allow: /core/*.js?
Allow: /core/*.gif
Allow: /core/*.jpg
Allow: /core/*.jpeg
Allow: /core/*.png
Allow: /core/*.svg
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /profiles/*.svg
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.txt
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /index.php/admin/
Disallow: /index.php/comment/reply/
Disallow: /index.php/filter/tips
Disallow: /index.php/node/add/
Disallow: /index.php/search/
Disallow: /index.php/user/password/
Disallow: /index.php/user/register/
Disallow: /index.php/user/login/
Disallow: /index.php/user/logout/
```

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: 2022/07/19

Plugin Output

tcp/443/www

```
Webmirror performed 18 queries in 3s (6.000 queries per second)

The following CGIs have been discovered :


+ CGI : /downloads
  Methods : GET
  Argument : field_file_category_target_id
  Argument : title
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

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

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/01/26, Modified: 2021/04/07

Plugin Output

tcp/80/www

```
URL     : http://lpps.sabah.gov.my/
Version : 1.15.12
source  : Server: nginx/1.15.12
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

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

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/01/26, Modified: 2021/04/07

Plugin Output

tcp/443/www

```
URL     : https://lpps.sabah.gov.my/
Version : 1.15.12
source  : Server: nginx/1.15.12
```