Lex_Retail Web Application Test

Report generated by Tenable Nessus™ Thu, 31 Jul 2025 14:20:48 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.8.250

8	12	18	0	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Jul 31 13:39:48 2025
End time: Thu Jul 31 14:20:48 2025

Host Information

IP: 192.168.8.250
OS: Windows 11

Vulnerabilities

201198 - Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.60 advisory.

- Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387)

- SSRF in Apache HTTP Server on Windows allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive UNCList to allow access during request processing. (CVE-2024-38472)

- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38473)

- Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag UnsafeAllow3F is specified. (CVE-2024-38474)

- Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag UnsafePrefixStat can be used to opt back in once ensuring the substitution is appropriately constrained.

(CVE-2024-38475)

- Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38476)

- null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38477)

- Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-39573)

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

Solution

Upgrade to Apache version 2.4.60 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

7.7

EPSS Score

0.9355

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)

STIG Severity

I

References

CVE	CVE-2024-36387
CVE	CVE-2024-38472
CVE	CVE-2024-38473
CVE	CVE-2024-38474
CVE	CVE-2024-38475
CVE	CVE-2024-38476
CVE	CVE-2024-38477
CVE	CVE-2024-39573
XREF	IAVA:2024-A-0378-S
XREF	CISA-KNOWN-EXPLOITED:2025/05/22

Plugin Information

Published: 2024/07/01, Modified: 2025/05/02

Plugin Output

tcp/80/www

```
URL               : http://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.60
```

201198 - Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.60 advisory.

- Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387)

- SSRF in Apache HTTP Server on Windows allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive UNCList to allow access during request processing. (CVE-2024-38472)

- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38473)

- Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag UnsafeAllow3F is specified. (CVE-2024-38474)

- Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag UnsafePrefixStat can be used to opt back in once ensuring the substitution is appropriately constrained.

(CVE-2024-38475)

- Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38476)

- null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38477)

- Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-39573)

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

Solution

Upgrade to Apache version 2.4.60 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

7.7

EPSS Score

0.9355

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)

STIG Severity

I

References

CVE	CVE-2024-36387
CVE	CVE-2024-38472
CVE	CVE-2024-38473
CVE	CVE-2024-38474
CVE	CVE-2024-38475
CVE	CVE-2024-38476
CVE	CVE-2024-38477
CVE	CVE-2024-39573
XREF	IAVA:2024-A-0378-S
XREF	CISA-KNOWN-EXPLOITED:2025/05/22

Plugin Information

Published: 2024/07/01, Modified: 2025/05/02

Plugin Output

tcp/443/www

```
URL               : https://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.60
```

201082 - OpenSSL 3.1.0 < 3.1.7 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 3.3.2 (Affected since 3.3.0). (CVE-2024-5535)

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?f87142a6

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.1.7 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.1077

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-5535

Plugin Information

Published: 2024/06/27, Modified: 2025/04/14

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.7
```

201082 - OpenSSL 3.1.0 < 3.1.7 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 3.3.2 (Affected since 3.3.0). (CVE-2024-5535)

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?f87142a6

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.1.7 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.1077

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-5535

Plugin Information

Published: 2024/06/27, Modified: 2025/04/14

Plugin Output

tcp/443/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.7
```

200162 - PHP 8.2.x < 8.2.20 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.20. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.20 advisory.

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use Best-Fit behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. (CVE-2024-4577)

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. (CVE-2024-5458)

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.

(CVE-2024-5585)

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-8.php#8.2.20

Solution

Upgrade to PHP version 8.2.20 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

9.6

EPSS Score

0.9441

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-4577
CVE	CVE-2024-5458
CVE	CVE-2024-5585
XREF	CISA-KNOWN-EXPLOITED:2024/07/03
XREF	IAVA:2024-A-0330-S

Exploitable With

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

Plugin Information

Published: 2024/06/06, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
  URL              : http://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
  Installed version : 8.2.12
  Fixed version     : 8.2.20
```

200162 - PHP 8.2.x < 8.2.20 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.20. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.20 advisory.

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use Best-Fit behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. (CVE-2024-4577)

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. (CVE-2024-5458)

- In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.

(CVE-2024-5585)

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-8.php#8.2.20

Solution

Upgrade to PHP version 8.2.20 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

9.6

EPSS Score

0.9441

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-4577
CVE	CVE-2024-5458
CVE	CVE-2024-5585
XREF	CISA-KNOWN-EXPLOITED:2024/07/03
XREF	IAVA:2024-A-0330-S

Exploitable With

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

Plugin Information

Published: 2024/06/06, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
  URL               : https://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
  Installed version : 8.2.12
  Fixed version     : 8.2.20
```

211671 - PHP 8.2.x < 8.2.26 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.26. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.26 advisory.

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

See Also

http://php.net/ChangeLog-8.php#8.2.26

https://github.com/php/php-src/security/advisories/GHSA-5hqh-c84r-qjcv

https://github.com/php/php-src/security/advisories/GHSA-c5f2-jwm7-mmq2

https://github.com/php/php-src/security/advisories/GHSA-g665-fm4p-vhff

https://github.com/php/php-src/security/advisories/GHSA-h35g-vwh6-m678

https://github.com/php/php-src/security/advisories/GHSA-r977-prxv-hc43

Solution

Upgrade to PHP version 8.2.26 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

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

VPR Score

6.7

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-8929
CVE	CVE-2024-8932
CVE	CVE-2024-11233
CVE	CVE-2024-11234
CVE	CVE-2024-11236
XREF	IAVA:2024-A-0763-S

Plugin Information

Published: 2024/11/21, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
 URL               : http://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.26
```

211671 - PHP 8.2.x < 8.2.26 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.26. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.26 advisory.

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

See Also

http://php.net/ChangeLog-8.php#8.2.26

https://github.com/php/php-src/security/advisories/GHSA-5hqh-c84r-qjcv

https://github.com/php/php-src/security/advisories/GHSA-c5f2-jwm7-mmq2

https://github.com/php/php-src/security/advisories/GHSA-g665-fm4p-vhff

https://github.com/php/php-src/security/advisories/GHSA-h35g-vwh6-m678

https://github.com/php/php-src/security/advisories/GHSA-r977-prxv-hc43

Solution

Upgrade to PHP version 8.2.26 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

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

VPR Score

6.7

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-8929
CVE	CVE-2024-8932
CVE	CVE-2024-11233
CVE	CVE-2024-11234
CVE	CVE-2024-11236
XREF	IAVA:2024-A-0763-S

Plugin Information

Published: 2024/11/21, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
 URL               : https://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.26
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/) (CVE-2024-27316)

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

Solution

Upgrade to Apache version 2.4.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.9036

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-38709
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/04/04, Modified: 2024/07/12

Plugin Output

tcp/80/www

```
URL               : http://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.59
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/) (CVE-2024-27316)

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

Solution

Upgrade to Apache version 2.4.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.9036

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-38709
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/04/04, Modified: 2024/07/12

Plugin Output

tcp/443/www

```
URL               : https://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.59
```

210450 - Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.62. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.62 advisory.

- SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. (CVE-2024-40898)

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.62 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0044

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-40898

Plugin Information

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

Plugin Output

tcp/80/www

```
URL               : http://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.62
```

210450 - Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.62. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.62 advisory.

- SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. (CVE-2024-40898)

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.62 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0044

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-40898

Plugin Information

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

Plugin Output

tcp/443/www

```
URL               : https://192.168.8.250/
Installed version : 2.4.58
Fixed version     : 2.4.62
```

183890 - OpenSSL 3.1.0 < 3.1.4 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.4. It is, therefore, affected by a vulnerability as referenced in the 3.1.4 advisory.

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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?442518e0

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.openssl.org/news/secadv/20231024.txt

https://www.openssl.org/policies/secpolicy.html

Solution

Upgrade to OpenSSL version 3.1.4 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0573

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5363
XREF	IAVA:2023-A-0582-S

Plugin Information

Published: 2023/10/25, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.4
```

183890 - OpenSSL 3.1.0 < 3.1.4 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.4. It is, therefore, affected by a vulnerability as referenced in the 3.1.4 advisory.

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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?442518e0

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.openssl.org/news/secadv/20231024.txt

https://www.openssl.org/policies/secpolicy.html

Solution

Upgrade to OpenSSL version 3.1.4 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0573

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5363
XREF	IAVA:2023-A-0582-S

Plugin Information

Published: 2023/10/25, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.4
```

192974 - OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.6. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.6 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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?5ee92eab

http://www.nessus.org/u?6f15218c

http://www.nessus.org/u?f40bd907

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

Solution

Upgrade to OpenSSL version 3.1.6 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 v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0165

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-2511
CVE	CVE-2024-4603
CVE	CVE-2024-4741
XREF	IAVA:2024-A-0208-S

Plugin Information

Published: 2024/04/08, Modified: 2024/11/14

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.6
```

192974 - OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.6. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.6 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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?5ee92eab

http://www.nessus.org/u?6f15218c

http://www.nessus.org/u?f40bd907

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

Solution

Upgrade to OpenSSL version 3.1.6 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 v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0165

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-2511
CVE	CVE-2024-4603
CVE	CVE-2024-4741
XREF	IAVA:2024-A-0208-S

Plugin Information

Published: 2024/04/08, Modified: 2024/11/14

Plugin Output

tcp/443/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.6
```

207822 - PHP 8.2.x < 8.2.24 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.24. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.24 advisory.

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using a certain non-standard configurations of Windows codepages, the fixes for CVE-2024-4577 https://github.com/advisories/GHSA-vxpp-6299-mxw3 may still be bypassed and the same command injection related to Windows Best Fit codepage behavior can be achieved. This may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. (CVE-2024-8926)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, erroneous parsing of multipart form data contained in an HTTP POST request could lead to legitimate data not being processed.

This could lead to malicious attacker able to control part of the submitted data being able to exclude portion of other data, potentially leading to erroneous application behavior. (CVE-2024-8925)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, HTTP_REDIRECT_STATUS variable is used to check whether or not CGI binary is being run by the HTTP server. However, in certain scenarios, the content of this variable can be controlled by the request submitter via HTTP headers, which can lead to cgi.force_redirect option not being correctly applied. In certain configurations this may lead to arbitrary file inclusion in PHP. (CVE-2024-8927)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using PHP-FPM SAPI and it is configured to catch workers output through catch_workers_output = yes, it may be possible to pollute the final log or remove up to 4 characters from the log messages by manipulating log message content.

Additionally, if PHP-FPM is configured to use syslog output, it may be possible to further remove log data using the same vulnerability. (CVE-2024-9026)

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-8.php#8.2.24

Solution

Upgrade to PHP version 8.2.24 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0217

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-8925
CVE	CVE-2024-8926
CVE	CVE-2024-8927
CVE	CVE-2024-9026
XREF	IAVA:2024-A-0609-S

Plugin Information

Published: 2024/09/26, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
  URL               : http://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
  Installed version : 8.2.12
  Fixed version     : 8.2.24
```

207822 - PHP 8.2.x < 8.2.24 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.24. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.24 advisory.

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using a certain non-standard configurations of Windows codepages, the fixes for CVE-2024-4577 https://github.com/advisories/GHSA-vxpp-6299-mxw3 may still be bypassed and the same command injection related to Windows Best Fit codepage behavior can be achieved. This may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. (CVE-2024-8926)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, erroneous parsing of multipart form data contained in an HTTP POST request could lead to legitimate data not being processed.

This could lead to malicious attacker able to control part of the submitted data being able to exclude portion of other data, potentially leading to erroneous application behavior. (CVE-2024-8925)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, HTTP_REDIRECT_STATUS variable is used to check whether or not CGI binary is being run by the HTTP server. However, in certain scenarios, the content of this variable can be controlled by the request submitter via HTTP headers, which can lead to cgi.force_redirect option not being correctly applied. In certain configurations this may lead to arbitrary file inclusion in PHP. (CVE-2024-8927)

- In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using PHP-FPM SAPI and it is configured to catch workers output through catch_workers_output = yes, it may be possible to pollute the final log or remove up to 4 characters from the log messages by manipulating log message content.

Additionally, if PHP-FPM is configured to use syslog output, it may be possible to further remove log data using the same vulnerability. (CVE-2024-9026)

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-8.php#8.2.24

Solution

Upgrade to PHP version 8.2.24 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0217

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-8925
CVE	CVE-2024-8926
CVE	CVE-2024-8927
CVE	CVE-2024-9026
XREF	IAVA:2024-A-0609-S

Plugin Information

Published: 2024/09/26, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
  URL              : https://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
  Installed version : 8.2.12
  Fixed version     : 8.2.24
```

232707 - PHP 8.2.x < 8.2.28 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.28. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.28 advisory.

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

See Also

http://php.net/ChangeLog-8.php#8.2.28

https://github.com/php/php-src/security/advisories/GHSA-52jp-hrpf-2jff

https://github.com/php/php-src/security/advisories/GHSA-hgf5-96fm-v528

https://github.com/php/php-src/security/advisories/GHSA-p3x9-6h7p-cgfc

https://github.com/php/php-src/security/advisories/GHSA-pcmh-g36c-qc44

https://github.com/php/php-src/security/advisories/GHSA-v8xr-gpvj-cx9g

Solution

Upgrade to PHP version 8.2.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.4

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-1217
CVE	CVE-2025-1219
CVE	CVE-2025-1734
CVE	CVE-2025-1736
CVE	CVE-2025-1861
XREF	IAVA:2025-A-0183

Plugin Information

Published: 2025/03/13, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
 URL               : http://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.28
```

232707 - PHP 8.2.x < 8.2.28 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.28. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.28 advisory.

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

See Also

http://php.net/ChangeLog-8.php#8.2.28

https://github.com/php/php-src/security/advisories/GHSA-52jp-hrpf-2jff

https://github.com/php/php-src/security/advisories/GHSA-hgf5-96fm-v528

https://github.com/php/php-src/security/advisories/GHSA-p3x9-6h7p-cgfc

https://github.com/php/php-src/security/advisories/GHSA-pcmh-g36c-qc44

https://github.com/php/php-src/security/advisories/GHSA-v8xr-gpvj-cx9g

Solution

Upgrade to PHP version 8.2.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.4

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-1217
CVE	CVE-2025-1219
CVE	CVE-2025-1734
CVE	CVE-2025-1736
CVE	CVE-2025-1861
XREF	IAVA:2025-A-0183

Plugin Information

Published: 2025/03/13, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
 URL               : https://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.28
```

10678 - Apache mod_info /server-info Information Disclosure

Synopsis

The remote web server discloses configuration information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

https://www.owasp.org/index.php/SCG_WS_Apache

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

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: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://192.168.8.250/server-info

Attached is a copy of the response
```

10678 - Apache mod_info /server-info Information Disclosure

Synopsis

The remote web server discloses configuration information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

https://www.owasp.org/index.php/SCG_WS_Apache

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

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: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/443/www

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

https://192.168.8.250/server-info

Attached is a copy of the response
```

10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses process information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

See Also

https://www.owasp.org/index.php/SCG_WS_Apache

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

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: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://192.168.8.250/server-status

Attached is a copy of the response
```

10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses process information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

See Also

https://www.owasp.org/index.php/SCG_WS_Apache

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

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: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/443/www

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

https://192.168.8.250/server-status

Attached is a copy of the response
```

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://192.168.8.250/dashboard/docs/
http://192.168.8.250/dashboard/docs/images/
http://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
http://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
http://192.168.8.250/dashboard/docs/images/auto-start-xampp/
http://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
http://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
http://192.168.8.250/dashboard/docs/images/configure-vhosts/
http://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
http://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
```

```
http://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
http://192.168.8.250/dashboard/docs/images/deploy-git-app/
http://192.168.8.250/dashboard/docs/images/install-wordpress/
http://192.168.8.250/dashboard/docs/images/reset-mysql-password/
http://192.168.8.250/dashboard/docs/images/send-mail/
http://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
http://192.168.8.250/dashboard/docs/images/troubleshoot-apache/
http://192.168.8.250/dashboard/docs/images/use-different-php-version/
http://192.168.8.250/dashboard/docs/images/use-php-fcgi/
http://192.168.8.250/dashboard/docs/images/use-sqlite/
http://192.168.8.250/dashboard/images/
http://192.168.8.250/dashboard/images/bitnami-xampp/
http://192.168.8.250/dashboard/images/blog/
http://192.168.8.250/dashboard/images/flags/
http://192.168.8.250/dashboard/images/screenshots/
http://192.168.8.250/dashboard/images/stamps/
http://192.168.8.250/dashboard/images/team/
http://192.168.8.250/dashboard/stylesheets/
http://192.168.8.250/img/
http://192.168.8.250/xampp/
```

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/443/www

```
The following directories are browsable :

https://192.168.8.250/dashboard/docs/
https://192.168.8.250/dashboard/docs/images/
https://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
https://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
https://192.168.8.250/dashboard/docs/images/auto-start-xampp/
https://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
https://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
https://192.168.8.250/dashboard/docs/images/configure-vhosts/
https://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
https://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
```

```
https://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
https://192.168.8.250/dashboard/docs/images/deploy-git-app/
https://192.168.8.250/dashboard/docs/images/install-wordpress/
https://192.168.8.250/dashboard/docs/images/reset-mysql-password/
https://192.168.8.250/dashboard/docs/images/send-mail/
https://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
https://192.168.8.250/dashboard/docs/images/troubleshoot-apache/
https://192.168.8.250/dashboard/docs/images/use-different-php-version/
https://192.168.8.250/dashboard/docs/images/use-php-fcgi/
https://192.168.8.250/dashboard/docs/images/use-sqlite/
https://192.168.8.250/dashboard/images/
https://192.168.8.250/dashboard/images/bitnami-xampp/
https://192.168.8.250/dashboard/images/blog/
https://192.168.8.250/dashboard/images/flags/
https://192.168.8.250/dashboard/images/screenshots/
https://192.168.8.250/dashboard/images/stamps/
https://192.168.8.250/dashboard/images/team/
https://192.168.8.250/dashboard/stylesheets/
https://192.168.8.250/img/
https://192.168.8.250/xampp/
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.0

EPSS Score

0.7993

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus673573856.html HTTP/1.1
Connection: Close
Host: 192.168.8.250
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Thu, 31 Jul 2025 17:44:39 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus673573856.html HTTP/1.1
Connection: Keep-Alive
```

```
Host: 192.168.8.250
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.0

EPSS Score

0.7993

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/443/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus1204871888.html HTTP/1.1
Connection: Close
Host: 192.168.8.250
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Thu, 31 Jul 2025 17:44:39 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1204871888.html HTTP/1.1
Connection: Keep-Alive
```

```
Host: 192.168.8.250
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

185161 - OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.5 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

- Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application.

The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678)

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?0a42ec4e

http://www.nessus.org/u?950a9188

http://www.nessus.org/u?aca829a1

http://www.nessus.org/u?d086a7ea

https://www.cve.org/CVERecord?id=CVE-2023-5678

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

Solution

Upgrade to OpenSSL version 3.1.5 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0274

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5678
CVE	CVE-2023-6129
CVE	CVE-2023-6237
CVE	CVE-2024-0727
XREF	IAVA:2024-A-0121-S

Plugin Information

Published: 2023/11/07, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.5
```

185161 - OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.5 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

- Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application.

The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678)

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?0a42ec4e

http://www.nessus.org/u?950a9188

http://www.nessus.org/u?aca829a1

http://www.nessus.org/u?d086a7ea

https://www.cve.org/CVERecord?id=CVE-2023-5678

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

Solution

Upgrade to OpenSSL version 3.1.5 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0274

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5678
CVE	CVE-2023-6129
CVE	CVE-2023-6237
CVE	CVE-2024-0727
XREF	IAVA:2024-A-0121-S

Plugin Information

Published: 2023/11/07, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.5
```

209154 - OpenSSL 3.1.0 < 3.1.8 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.8. It is, therefore, affected by a vulnerability as referenced in the 3.1.8 advisory.

- Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only named curves are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an exotic curve encoding. The affected APIs include:

EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions.

Applications working with exotic explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

(CVE-2024-9143)

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?5f636435

https://openssl-library.org/news/secadv/20241016.txt

https://openssl-library.org/policies/general/security-policy/#low

https://www.cve.org/CVERecord?id=CVE-2024-9143

Solution

Upgrade to OpenSSL version 3.1.8 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0036

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)

STIG Severity

I

References

CVE	CVE-2024-9143
XREF	IAVA:2025-A-0127-S

Plugin Information

Published: 2024/10/16, Modified: 2025/05/23

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.8
```

209154 - OpenSSL 3.1.0 < 3.1.8 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.8. It is, therefore, affected by a vulnerability as referenced in the 3.1.8 advisory.

- Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only named curves are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an exotic curve encoding. The affected APIs include:

EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions.

Applications working with exotic explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

(CVE-2024-9143)

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?5f636435

https://openssl-library.org/news/secadv/20241016.txt

https://openssl-library.org/policies/general/security-policy/#low

https://www.cve.org/CVERecord?id=CVE-2024-9143

Solution

Upgrade to OpenSSL version 3.1.8 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0036

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)

STIG Severity

I

References

CVE	CVE-2024-9143
XREF	IAVA:2025-A-0127-S

Plugin Information

Published: 2024/10/16, Modified: 2025/05/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version : 3.1.3
Fixed version    : 3.1.8
```

193191 - PHP 8.2.x < 8.2.18 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.18. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.18 advisory.

- In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. (CVE-2022-31629)

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-8.php#8.2.18

Solution

Upgrade to PHP version 8.2.18 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.3

EPSS Score

0.5461

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-31629
CVE	CVE-2024-1874
CVE	CVE-2024-2756
CVE	CVE-2024-3096
XREF	IAVA:2024-A-0244-S

Plugin Information

Published: 2024/04/11, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
 URL               : http://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.18
```

193191 - PHP 8.2.x < 8.2.18 Multiple Vulnerabilities

Synopsis

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

Description

The version of PHP installed on the remote host is prior to 8.2.18. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.2.18 advisory.

- In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. (CVE-2022-31629)

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-8.php#8.2.18

Solution

Upgrade to PHP version 8.2.18 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.3

EPSS Score

0.5461

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-31629
CVE	CVE-2024-1874
CVE	CVE-2024-2756
CVE	CVE-2024-3096
XREF	IAVA:2024-A-0244-S

Plugin Information

Published: 2024/04/11, Modified: 2025/05/26

Plugin Output

tcp/443/www

```
 URL              : https://192.168.8.250/ (8.2.12 under Server: Apache/2.4.58 (Win64)
OpenSSL/3.1.3 PHP/8.2.12, X-Powered-By: PHP/8.2.12)
 Installed version : 8.2.12
 Fixed version     : 8.2.18
```

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://192.168.8.250/dashboard/phpinfo.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

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/443/www

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

  https://192.168.8.250/dashboard/phpinfo.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

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://192.168.8.250/phpmyadmin/doc/html/
  - http://192.168.8.250/phpmyadmin/doc/html/bookmarks.html
  - http://192.168.8.250/phpmyadmin/doc/html/charts.html
  - http://192.168.8.250/phpmyadmin/doc/html/copyright.html
  - http://192.168.8.250/phpmyadmin/doc/html/credits.html
  - http://192.168.8.250/phpmyadmin/doc/html/developers.html
  - http://192.168.8.250/phpmyadmin/doc/html/genindex.html
  - http://192.168.8.250/phpmyadmin/doc/html/glossary.html
  - http://192.168.8.250/phpmyadmin/doc/html/import_export.html
  - http://192.168.8.250/phpmyadmin/doc/html/index.html
  - http://192.168.8.250/phpmyadmin/doc/html/intro.html
  - http://192.168.8.250/phpmyadmin/doc/html/other.html
  - http://192.168.8.250/phpmyadmin/doc/html/privileges.html
  - http://192.168.8.250/phpmyadmin/doc/html/relations.html
  - http://192.168.8.250/phpmyadmin/doc/html/require.html
  - http://192.168.8.250/phpmyadmin/doc/html/search.html
  - http://192.168.8.250/phpmyadmin/doc/html/security.html
  - http://192.168.8.250/phpmyadmin/doc/html/settings.html
  - http://192.168.8.250/phpmyadmin/doc/html/setup.html
  - http://192.168.8.250/phpmyadmin/doc/html/themes.html
  - http://192.168.8.250/phpmyadmin/doc/html/transformations.html
  - http://192.168.8.250/phpmyadmin/doc/html/two_factor.html
  - http://192.168.8.250/phpmyadmin/doc/html/user.html
  - http://192.168.8.250/phpmyadmin/doc/html/vendors.html
```

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/443/www

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

  - https://192.168.8.250/phpmyadmin/doc/html/
  - https://192.168.8.250/phpmyadmin/doc/html/bookmarks.html
  - https://192.168.8.250/phpmyadmin/doc/html/charts.html
  - https://192.168.8.250/phpmyadmin/doc/html/copyright.html
  - https://192.168.8.250/phpmyadmin/doc/html/credits.html
  - https://192.168.8.250/phpmyadmin/doc/html/developers.html
  - https://192.168.8.250/phpmyadmin/doc/html/genindex.html
  - https://192.168.8.250/phpmyadmin/doc/html/glossary.html
  - https://192.168.8.250/phpmyadmin/doc/html/import_export.html
  - https://192.168.8.250/phpmyadmin/doc/html/index.html
  - https://192.168.8.250/phpmyadmin/doc/html/intro.html
  - https://192.168.8.250/phpmyadmin/doc/html/other.html
  - https://192.168.8.250/phpmyadmin/doc/html/privileges.html
  - https://192.168.8.250/phpmyadmin/doc/html/relations.html
  - https://192.168.8.250/phpmyadmin/doc/html/require.html
  - https://192.168.8.250/phpmyadmin/doc/html/search.html
  - https://192.168.8.250/phpmyadmin/doc/html/security.html
  - https://192.168.8.250/phpmyadmin/doc/html/settings.html
  - https://192.168.8.250/phpmyadmin/doc/html/setup.html
  - https://192.168.8.250/phpmyadmin/doc/html/themes.html
  - https://192.168.8.250/phpmyadmin/doc/html/transformations.html
  - https://192.168.8.250/phpmyadmin/doc/html/two_factor.html
  - https://192.168.8.250/phpmyadmin/doc/html/user.html
  - https://192.168.8.250/phpmyadmin/doc/html/vendors.html
```

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://192.168.8.250/
Version    : 2.4.58
Source     : Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
backported : 0
modules    : OpenSSL/3.1.3 PHP/8.2.12
os         : Win64
```

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/443/www

```
URL        : https://192.168.8.250/
Version    : 2.4.58
Source     : Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
backported : 0
modules    : OpenSSL/3.1.3 PHP/8.2.12
os         : Win64
```

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 'set_theme' parameter of the /phpmyadmin/index.php?route=/themes/set CGI :

/phpmyadmin/index.php?route=/themes/set?set_theme=%00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2Fthemes&#x25;2Fset&#x2
5;3Fset_theme&#x25;3D&#x25;00qtzkmj&amp;server&#x3D;1&amp;lang&#x3D;en"
class="config-form disableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------
```

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

/phpmyadmin/index.php?route=/?lang=%00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2F&#x25;3Flang&#x25;3D&
#x25;00qtzkmj&amp;server&#x3D;1&amp;lang&#x3D;en" class="config-form dis
ableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------

+ The 'collation_connection' parameter of the /phpmyadmin/index.php?route=/collation-connection
 CGI :

/phpmyadmin/index.php?route=/collation-connection?collation_connection=%
00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2Fcollation-connection&
#x25;3Fcollation_connection&#x25;3D&#x25;00qtzkmj&amp;server&#x3D;1&amp;
lang&#x3D;en" class="config-form disableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------

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

/phpmyadmin/index.php?route=%00qtzkmj

------- [...]
```

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/443/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'set_theme' parameter of the /phpmyadmin/index.php?route=/themes/set CGI :

/phpmyadmin/index.php?route=/themes/set?set_theme=%00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2Fthemes&#x25;2Fset&#x2
5;3Fset_theme&#x25;3D&#x25;00qtzkmj&amp;server&#x3D;1&amp;lang&#x3D;en"
class="config-form disableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------
```

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

/phpmyadmin/index.php?route=/?lang=%00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2F&#x25;3Flang&#x25;3D&
#x25;00qtzkmj&amp;server&#x3D;1&amp;lang&#x3D;en" class="config-form dis
ableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------

+ The 'collation_connection' parameter of the /phpmyadmin/index.php?route=/collation-connection
 CGI :

/phpmyadmin/index.php?route=/collation-connection?collation_connection=%
00qtzkmj

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

<div id="pma_navi_settings_container">
<div id="pma_navigation_settings"><div class="page_settings"><form metho
d="post" action="index.php&#x3F;route&#x3D;&#x25;2Fcollation-connection&
#x25;3Fcollation_connection&#x25;3D&#x25;00qtzkmj&amp;server&#x3D;1&amp;
lang&#x3D;en" class="config-form disableAjax">
<input type="hidden" name="tab_hash" value="">
<input type="hidden" name="check_page_refresh" id="check_page_refr [...]
------------------------

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

/phpmyadmin/index.php?route=%00qtzkmj

------- [...]
```

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=4          SP=4         AP=4         SC=4         AC=4

SQL injection                            : S=1224       SP=1224      AP=23400     SC=120
 AC=>2G
unseen parameters                        : S=1785       SP=1785      AP=34125     SC=175
 AC=402653464
local file inclusion                     : S=51         SP=51        AP=975       SC=5
 AC=134217736
web code injection                       : S=51         SP=51        AP=975       SC=5
 AC=134217736
XML injection                            : S=51         SP=51        AP=975       SC=5
 AC=134217736
format string                            : S=102        SP=102       AP=1950      SC=10
 AC=268435472
script injection                         : S=4          SP=4         AP=4         SC=4         AC=4

cross-site scripting (comprehensive test): S=204        SP=204       AP=3900      SC=20
 AC=536870944
```

```
injectable parameter                      : S=102        SP=102       AP=1950      SC=10
 AC=268435472
cross-site scripting (extended patterns) : S=24         SP=24        AP=24        SC=24        AC=24

directory traversal (write access)       : S=102        SP=102       AP=1950      SC=10
 AC=268435472
SSI injection                            : S=153        SP=153       AP=2925      SC=15
 AC=402653208
header injection                         : S=8          SP=8         AP=8         SC=8         AC=8

HTML injection                           : S=20         SP=20        AP=20        SC=20        AC=20

directory traversal                      : S=1275       SP=1275      AP=24375     SC=125
 AC=>2G
arbitrary command execution (time based) : S=306        SP=306       AP=5850      SC=30
 AC=805306416
persistent XSS                          [...]
```

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=204        SP=204       AP=3900      SC=20
 AC=536870944
persistent XSS                           : S=204        SP=204       AP=3900      SC=20
 AC=536870944
arbitrary command execution              : S=816        SP=816       AP=15600     SC=80
 AC=>2G
web code injection                       : S=51         SP=51        AP=975       SC=5
 AC=134217736
script injection                         : S=4          SP=4         AP=4         SC=4         AC=4

HTML injection                           : S=20         SP=20        AP=20        SC=20        AC=20

arbitrary command execution (time based) : S=306        SP=306       AP=5850      SC=30
 AC=805306416
XML injection                            : S=51         SP=51        AP=975       SC=5
 AC=134217736
unseen parameters                        : S=1785       SP=1785      AP=34125     SC=175
 AC=402653464
```

```
directory traversal (write access)        : S=102        SP=102       AP=1950      SC=10
 AC=268435472
SQL injection (2nd order)                 : S=51         SP=51        AP=975       SC=5
 AC=134217736
on site request forgery                   : S=4          SP=4         AP=4         SC=4         AC=4

blind SQL injection (4 requests)          : S=204        SP=204       AP=3900      SC=20
 AC=536870944
HTTP response splitting                   : S=36         SP=36        AP=36        SC=36        AC=36

directory traversal (extended test)       : S=2601       SP=2601      AP=49725     SC=255
 AC=>2G
header injection                          : S=8          SP=8         AP=8         SC=8         AC=8

injectable parameter                      : S=102        SP=102       AP=1950      SC=10
 AC=268435472
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/80/www

```
The following tests timed out without finding any flaw :
- SQL injection (on parameters names)
- SQL injection
- directory traversal
- cross-site scripting (comprehensive test)
- SQL injection (2nd order)
- blind SQL injection
- blind SQL injection (time based)
- local file inclusion
- arbitrary command execution
```

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
- SQL injection (2nd order)
- blind SQL injection
- blind SQL injection (time based)
- cross-site scripting (comprehensive test)
- directory traversal
```

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8000/www

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8089/www

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

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


http://app01.localhost                  -
http://app02.localhost                  -
http://cdnjs.cloudflare.com/ajax/libs/font-awesome/3.1.0/css/font-awesome.min.css - /dashboard/
http://client1/                         -
http://client2/                         -
http://code.google.com/p/gitextensions/ -
http://framework.zend.com/              -
http://framework.zend.com/downloads/latest -
http://framework.zend.com/manual/1.12/en/learning.html -
http://framework.zend.com/manual/2.3/en/user-guide/overview.html -
http://git-extensions-documentation.readthedocs.org/en/latest/getting_started.html -
http://git-scm.com/                     -
http://git-scm.com/book                 -
http://git-scm.com/download/win         -
http://localhost                        -
http://localhost/Slim                   -
http://localhost/example.php            -
http://localhost/example/phpmailer.php  -
http://localhost/myapp                  -
http://localhost/myapp/                 -
http://localhost/phpMyAdmin             -
http://localhost/sendmail.php           -
http://localhost/sqlite.php             -
http://localhost/wordpress              -
http://localhost/xampp/phpinfo.php      -
http://localhost:8080/                  -
http://myhost                           -
```

```
http://phpmailer.worxware.com/          -
http://sourceforge.net/projects/wincachegrind/ -
http://sqlite.org/docs/                 -
http://support.microsoft.com/kb/841290  -
http://wordpress.localhost              -
http://www.apachelounge.com/download/   -
http://www.famfamfam.com/lab/icons/silk/ -
http://www.fastly.com/                  -
http://www.fpdf.org/                    -
http://www.jqplot.com/                  -
http://www.kaspersky.com/virusscanner   -
http://www.php-editors.com/articles/sql_phpmyadmin.php -
http://www.php.net/                     -
http://www.phpmyadmin.net/              -
http://www.sli [...]
```

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

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


http://app01.localhost                  - /dashboard/docs/configure-vhosts.html
http://app02.localhost                  - /dashboard/docs/configure-vhosts.html
http://client1/                         - /dashboard/docs/configure-vhosts.html
http://client2/                         - /dashboard/docs/configure-vhosts.html
http://code.google.com/p/gitextensions/ - /dashboard/docs/deploy-git-app.html
http://framework.zend.com/              - /dashboard/docs/create-framework-project-zf1.html
http://framework.zend.com/downloads/latest - /dashboard/docs/create-framework-project-zf1.html
http://framework.zend.com/manual/1.12/en/learning.html - /dashboard/docs/create-framework-project-
zf1.html
http://framework.zend.com/manual/2.3/en/user-guide/overview.html - /dashboard/docs/create-framework-
project-zf2.html
http://git-extensions-documentation.readthedocs.org/en/latest/getting_started.html - /dashboard/
docs/deploy-git-app.html
http://git-scm.com/                     - /dashboard/docs/deploy-git-app.html
http://git-scm.com/book                 - /dashboard/docs/deploy-git-app.html
http://git-scm.com/download/win         - /dashboard/docs/create-framework-project-zf2.html
http://localhost                        - /dashboard/docs/troubleshoot-apache.html
http://localhost/Slim                   - /dashboard/docs/deploy-git-app.html
http://localhost/example.php            - /dashboard/docs/transfer-files-ftp.html
http://localhost/example/phpmailer.php  - /dashboard/docs/send-mail.html
http://localhost/myapp                  - /dashboard/docs/create-framework-project-zf1.html
http://localhost/myapp/                 - /dashboard/docs/create-framework-project-zf1.html
http://localhost/phpMyAdmin             - /dashboard/docs/backup-restore-mysql.html
http://localhost/sendmail.php           - /dashboard/docs/send-mail.html
http://localhost/sqlite.php             - /dashboard/docs/use-sqlite.html
http://localhost/wordpress     [...]
```

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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 302 Found
Date: Thu, 31 Jul 2025 17:42:53 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Location: https://192.168.8.250/dashboard/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

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

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies have the 'secure' property enabled, despite being served over HTTP :

  Domain   :
  Path     : /phpmyadmin/
  Name     : phpMyAdmin_https
  Value    : 4cn7l6dce2359ua1oqtfoh1d2n
  Secure   : true
  HttpOnly : true
```

```
Domain   :
Path     : /phpmyadmin/
Name     : pma_lang_https
Value    : en
Secure   : true
HttpOnly : true
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies do not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /phpmyadmin/
  Name     : phpMyAdmin
  Value    : 14qclopb84f95d1c0una2147bi
  Secure   : false
  HttpOnly : true
```

```
Domain   :
Path     : /phpmyadmin/
Name     : pma_lang
Value    : en
Secure   : false
HttpOnly : true
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/8000/www

```
The following cookies have the 'secure' property enabled, despite being served over HTTP :

  Domain   :
  Path     : /phpmyadmin/
  Name     : phpMyAdmin_https
  Value    : 4cn7l6dce2359ua1oqtfoh1d2n
  Secure   : true
  HttpOnly : true
```

```
Domain   :
Path     : /phpmyadmin/
Name     : pma_lang_https
Value    : en
Secure   : true
HttpOnly : true
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/8089/www

```
The following cookies do not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /phpmyadmin/
  Name     : phpMyAdmin
  Value    : 14qclopb84f95d1c0una2147bi
  Secure   : false
  HttpOnly : true
```

```
Domain   :
Path     : /phpmyadmin/
Name     : pma_lang
Value    : en
Secure   : false
HttpOnly : true
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

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

    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/auto-start-xampp
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-use-tomcat
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /icons
    /img
    /server-info
    /server-status
    /webalizer
    /xampp


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 :

    /cgi-bin

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

    /
    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/auto-start-xampp
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-use-tomcat
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-m [...]
```

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 GET HEAD OPTIONS POST TRACE are allowed on :

    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/auto-start-xampp
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-use-tomcat
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /icons
    /img
    /server-info
    /server-status
    /webalizer
    /xampp


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 :

    /cgi-bin

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

    /
    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/auto-start-xampp
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-use-tomcat
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-m [...]
```

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/8000/www

```
Based on tests of each method :

  - HTTP methods DELETE GET HEAD OPTIONS PATCH POST PUT
    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/8089/www

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

  - HTTP methods GET HEAD OPTIONS are allowed on :

    /

Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS 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/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
```

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

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
```

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

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8000/www

```
The remote web server type is :

Splunkd
```

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/8089/www

```
The remote web server type is :

Splunkd
```

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/1.1 302 Found

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: Thu, 31 Jul 2025 17:48:26 GMT
  Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
  X-Powered-By: PHP/8.2.12
  Location: http://192.168.8.250/dashboard/
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :
```

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/443/www

```
Response Code : HTTP/1.1 302 Found

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

  Date: Thu, 31 Jul 2025 17:48:26 GMT
  Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
  X-Powered-By: PHP/8.2.12
  Location: https://192.168.8.250/dashboard/
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :
```

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://192.168.8.250/
HTTP response   : HTTP/1.1 302 Found
Redirect to     : http://192.168.8.250/dashboard/
Redirect type   : 30x redirect

Final page      : http://192.168.8.250/dashboard/
HTTP response   : HTTP/1.1 200 OK
```

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/443/www

```
  Request         : https://192.168.8.250/
  HTTP response   : HTTP/1.1 302 Found
  Redirect to     : https://192.168.8.250/dashboard/
  Redirect type   : 30x redirect


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

tcp/443/www

```
  Request         : https://192.168.8.250/
  HTTP response   : HTTP/1.1 302 Found
  Redirect to     : https://192.168.8.250/dashboard/
  Redirect type   : 30x redirect

  Final page      : https://192.168.8.250/dashboard/
  HTTP response   : HTTP/1.1 200 OK
```

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://192.168.8.250/dashboard/
  - http://192.168.8.250/dashboard/docs/
  - http://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - http://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - http://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - http://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - http://192.168.8.250/dashboard/docs/configure-vhosts.html
  - http://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
  - http://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
```

```
- http://192.168.8.250/dashboard/docs/create-framework-project-zf2.html
- http://192.168.8.250/dashboard/docs/deploy-git-app.html
- http://192.168.8.250/dashboard/docs/images/
- http://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
- http://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
- http://192.168.8.250/dashboard/docs/images/auto-start-xampp/
- http://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
- http://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
- http://192.168.8.250/dashboard/docs/images/configure-vhosts/
- http://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
- http://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
- http://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
- http://192.168.8.250/dashboard/docs/images/deploy-git-app/
- http://192.168.8.250/dashboard/docs/images/install-wordpress/
- http://192.168.8.250/dashboard/docs/images/reset-mysql-password/
- http://192.168.8.250/dashboard/docs/images/send-mail/
- http://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
- http://192.168.8.250/dashboard/docs/images/troubleshoot-apache/
- http://192.168.8.250/das [...]
```

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://192.168.8.250/dashboard/
  - https://192.168.8.250/dashboard/docs/
  - https://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - https://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - https://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - https://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - https://192.168.8.250/dashboard/docs/configure-vhosts.html
  - https://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
  - https://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
```

```
- https://192.168.8.250/dashboard/docs/create-framework-project-zf2.html
- https://192.168.8.250/dashboard/docs/deploy-git-app.html
- https://192.168.8.250/dashboard/docs/images/
- https://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
- https://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
- https://192.168.8.250/dashboard/docs/images/auto-start-xampp/
- https://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
- https://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
- https://192.168.8.250/dashboard/docs/images/configure-vhosts/
- https://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
- https://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
- https://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
- https://192.168.8.250/dashboard/docs/images/deploy-git-app/
- https://192.168.8.250/dashboard/docs/images/install-wordpress/
- https://192.168.8.250/dashboard/docs/images/reset-mysql-password/
- https://192.168.8.250/dashboard/docs/images/send-mail/
- https://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
- https://192.168.8.250/dashboard/docs/images/troubleshoot-apache/ [...]
```

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://192.168.8.250/dashboard/
  - http://192.168.8.250/dashboard/docs/
  - http://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - http://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - http://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - http://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - http://192.168.8.250/dashboard/docs/configure-vhosts.html
  - http://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
  - http://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
  - http://192.168.8.250/dashboard/docs/create-framework-project-zf2.html
  - http://192.168.8.250/dashboard/docs/deploy-git-app.html
  - http://192.168.8.250/dashboard/docs/images/
  - http://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
  - http://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
```

```
- http://192.168.8.250/dashboard/docs/images/auto-start-xampp/
- http://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
- http://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
- http://192.168.8.250/dashboard/docs/images/configure-vhosts/
- http://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
- http://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
- http://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
- http://192.168.8.250/dashboard/docs/images/deploy-git-app/
- http://192.168.8.250/dashboard/docs/images/install-wordpress/
- http://192.168.8.250/dashboard/docs/images/reset-mysql-password/
- http://192.168.8.250/dashboard/docs/images/send-mail/
- http://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
- http://192.168.8.250/dashboard/docs/images/troubleshoot-apache/
- http://192.168.8.250/dashboard/docs/images/use-d [...]
```

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/443/www

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

  - https://192.168.8.250/dashboard/
  - https://192.168.8.250/dashboard/docs/
  - https://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - https://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - https://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - https://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - https://192.168.8.250/dashboard/docs/configure-vhosts.html
  - https://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
  - https://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
  - https://192.168.8.250/dashboard/docs/create-framework-project-zf2.html
  - https://192.168.8.250/dashboard/docs/deploy-git-app.html
  - https://192.168.8.250/dashboard/docs/images/
  - https://192.168.8.250/dashboard/docs/images/access-phpmyadmin-remotely/
  - https://192.168.8.250/dashboard/docs/images/activate-use-xdebug/
```

```
- https://192.168.8.250/dashboard/docs/images/auto-start-xampp/
- https://192.168.8.250/dashboard/docs/images/backup-restore-mysql/
- https://192.168.8.250/dashboard/docs/images/configure-use-tomcat/
- https://192.168.8.250/dashboard/docs/images/configure-vhosts/
- https://192.168.8.250/dashboard/docs/images/configure-wildcard-subdomains/
- https://192.168.8.250/dashboard/docs/images/create-framework-project-zf1/
- https://192.168.8.250/dashboard/docs/images/create-framework-project-zf2/
- https://192.168.8.250/dashboard/docs/images/deploy-git-app/
- https://192.168.8.250/dashboard/docs/images/install-wordpress/
- https://192.168.8.250/dashboard/docs/images/reset-mysql-password/
- https://192.168.8.250/dashboard/docs/images/send-mail/
- https://192.168.8.250/dashboard/docs/images/transfer-files-ftp/
- https://192.168.8.250/dashboard/docs/images/troubleshoot-apache/
- https://192.168.8.2 [...]
```

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: 2025/02/12

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: 2025/02/12

Plugin Output

tcp/135/epmap

```
Port 135/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: 2025/02/12

Plugin Output

tcp/139/smb

```
Port 139/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: 2025/02/12

Plugin Output

tcp/443/www

```
Port 443/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: 2025/02/12

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: 2025/02/12

Plugin Output

tcp/902/vmware_auth

```
Port 902/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: 2025/02/12

Plugin Output

tcp/912/vmware_auth

```
Port 912/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: 2025/02/12

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: 2025/02/12

Plugin Output

tcp/8000/www

```
Port 8000/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: 2025/02/12

Plugin Output

tcp/8089/www

```
Port 8089/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: 2025/02/12

Plugin Output

tcp/8191

```
Port 8191/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: 2025/02/12

Plugin Output

tcp/9997

```
Port 9997/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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202506272001
Scanner edition used : Nessus Home

ERROR: Your plugins have not been updated since 2025/6/27
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
```

```
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Lex_Retail Web Application Test
Scan policy used : Web Application Tests
Scanner IP : 192.168.109.130
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 14.980 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : 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 : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/7/31 13:40 EDT (UTC -04:00)
Scan duration : 2430 sec
Scan for malware : no
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2024/11/14

Plugin Output

tcp/80/www

```
Source              : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version    : 3.1.3
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2024/11/14

Plugin Output

tcp/443/www

```
Source              : Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Reported version    : 3.1.3
```

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: 2025/05/26

Plugin Output

tcp/80/www

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

  Version : 8.2.12
  Source  : Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
  Source  : X-Powered-By: PHP/8.2.12
```

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: 2025/05/26

Plugin Output

tcp/443/www

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

  Version : 8.2.12
  Source  : Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
  Source  : X-Powered-By: PHP/8.2.12
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/06/10

Plugin Output

tcp/0

```
. You need to take the following 3 actions :

[ Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows) (210450) ]

+ Action to take : Upgrade to Apache version 2.4.62 or later.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).


[ OpenSSL 3.1.0 < 3.1.8 Vulnerability (209154) ]

+ Action to take : Upgrade to OpenSSL version 3.1.8 or later.

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


[ PHP 8.2.x < 8.2.28 Multiple Vulnerabilities (232707) ]

+ Action to take : Upgrade to PHP version 8.2.28 or later.

+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).
```

49069 - Splunk Management API Detection

Synopsis

An infrastructure monitoring tool is running on the remote host.

Description

The remote web server is an instance of the Splunk management API.
Splunk is a search, monitoring, and reporting tool for system administrators.

See Also

https://www.splunk.com/en_us/software.html
http://dev.splunk.com/restapi
http://www.nessus.org/u?3aa0f4e2
https://www.splunk.com/en_us/download/universal-forwarder.html

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

References

XREF IAVT:0001-T-0722

Plugin Information

Published: 2010/09/01, Modified: 2022/10/12

Plugin Output

tcp/8089/www

```
URL            : https://192.168.8.250:8089/
Version        : 9.4.2
Build          : e9664af3d956
Management API : 1
```

47619 - Splunk Web Detection

Synopsis

An infrastructure monitoring tool is running on the remote host.

Description

The web interface for Splunk is running on the remote host. Splunk is a search, monitoring, and reporting tool for system administrators.

Note that HTTP Basic Authentication credentials may be required to retrieve version information for some recent Splunk releases.

See Also

https://www.splunk.com/en_us/software.html

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0723

Plugin Information

Published: 2010/07/07, Modified: 2025/04/02

Plugin Output

tcp/8000/www

```
URL           : http://192.168.8.250:8000/
Version       : 9.4.2
License       : Enterprise
Web interface : 1
```

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 : Sat, 30 Aug 2025 17:43:52 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : 14qclopb84f95d1c0una2147bi
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/443/www

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

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Sat, 30 Aug 2025 17:43:52 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : 14qclopb84f95d1c0una2147bi
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/8000/www

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

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Sat, 30 Aug 2025 17:43:52 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : 14qclopb84f95d1c0una2147bi
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/8089/www

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

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Sat, 30 Aug 2025 17:43:52 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : 14qclopb84f95d1c0una2147bi
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

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://192.168.8.250/dashboard/
  - http://192.168.8.250/dashboard/docs/
  - http://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.pdf
  - http://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.pdfmarks
  - http://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - http://192.168.8.250/dashboard/docs/activate-use-xdebug.pdf
  - http://192.168.8.250/dashboard/docs/activate-use-xdebug.pdfmarks
  - http://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - http://192.168.8.250/dashboard/docs/auto-start-xampp.pdf
  - http://192.168.8.250/dashboard/docs/auto-start-xampp.pdfmarks
  - http://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - http://192.168.8.250/dashboard/docs/backup-restore-mysql.pdf
  - http://192.168.8.250/dashboard/docs/backup-restore-mysql.pdfmarks
  - http://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.8.250/dashboard/docs/change-mysql-temp-dir.pdf
  - http://192.168.8.250/dashboard/docs/change-mysql-temp-dir.pdfmarks
  - http://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - http://192.168.8.250/dashboard/docs/configure-use-tomcat.pdf
  - http://192.168.8.250/dashboard/docs/configure-use-tomcat.pdfmarks
  - http://192.168.8.250/dashboard/docs/configure-vhosts.html
  - http://192.168.8.250/dashboard/docs/configure-vhosts.pdf
```

```
- http://192.168.8.250/dashboard/docs/configure-vhosts.pdfmarks
- http://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
- http://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.pdf
- http://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.pdfmarks
- http://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
- http://192.168.8.250/dashboard/docs/create-framework-project-zf1.pdf
- http://192.168.8.250/dashboard/docs/create-framework-project-zf1.pdfmarks
- http://192.168.8.250/dashb [...]
```

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://192.168.8.250/dashboard/
  - https://192.168.8.250/dashboard/docs/
  - https://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.pdf
  - https://192.168.8.250/dashboard/docs/access-phpmyadmin-remotely.pdfmarks
  - https://192.168.8.250/dashboard/docs/activate-use-xdebug.html
  - https://192.168.8.250/dashboard/docs/activate-use-xdebug.pdf
  - https://192.168.8.250/dashboard/docs/activate-use-xdebug.pdfmarks
  - https://192.168.8.250/dashboard/docs/auto-start-xampp.html
  - https://192.168.8.250/dashboard/docs/auto-start-xampp.pdf
  - https://192.168.8.250/dashboard/docs/auto-start-xampp.pdfmarks
  - https://192.168.8.250/dashboard/docs/backup-restore-mysql.html
  - https://192.168.8.250/dashboard/docs/backup-restore-mysql.pdf
  - https://192.168.8.250/dashboard/docs/backup-restore-mysql.pdfmarks
  - https://192.168.8.250/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.8.250/dashboard/docs/change-mysql-temp-dir.pdf
  - https://192.168.8.250/dashboard/docs/change-mysql-temp-dir.pdfmarks
  - https://192.168.8.250/dashboard/docs/configure-use-tomcat.html
  - https://192.168.8.250/dashboard/docs/configure-use-tomcat.pdf
  - https://192.168.8.250/dashboard/docs/configure-use-tomcat.pdfmarks
  - https://192.168.8.250/dashboard/docs/configure-vhosts.html
  - https://192.168.8.250/dashboard/docs/configure-vhosts.pdf
```

```
    - https://192.168.8.250/dashboard/docs/configure-vhosts.pdfmarks
    - https://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.html
    - https://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.pdf
    - https://192.168.8.250/dashboard/docs/configure-wildcard-subdomains.pdfmarks
    - https://192.168.8.250/dashboard/docs/create-framework-project-zf1.html
    - https://192.168.8.250/dashboard/docs/create-framework-project-zf1.pdf
    - https://192.168.8.250/dashboard/docs/create-framework-project-zf1.pdfmarks
    [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/cgi-bin, /webalizer, /icons, /img, /server-info, /server-status, /xampp, /phpmyadmin

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/443/www

```
The following directories were discovered:
/cgi-bin, /webalizer, /icons, /img, /server-info, /server-status, /xampp, /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
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```
The following email address has been gathered :

- 'security%40phpmyadmin.net', referenced from :
   /phpmyadmin/doc/html/security.html
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/443/www

```
The following email address has been gathered :

- 'security%40phpmyadmin.net', referenced from :
   /phpmyadmin/doc/html/security.html
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

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

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /dashboard/docs/access-phpmyadmin-remotely.pdf
    /dashboard/docs/activate-use-xdebug.pdf
    /dashboard/docs/create-framework-project-zf1.pdf
    /dashboard/docs/create-framework-project-zf2.pdf
    /dashboard/docs/deploy-git-app.pdf
    /dashboard/docs/increase-php-file-upload-limit.pdf
    /dashboard/docs/reset-mysql-password.pdf
    /dashboard/docs/send-mail.pdf
    /dashboard/docs/use-sqlite.pdf
    /dashboard/docs/use-php-fcgi.pdf
    /dashboard/docs/use-different-php-version.pdf
    /dashboard/docs/troubleshoot-apache.pdf
    /dashboard/docs/transfer-files-ftp.pdf
    /dashboard/docs/configure-wildcard-subdomains.pdf
    /dashboard/docs/configure-vhosts.pdf
    /dashboard/docs/configure-use-tomcat.pdf
    /dashboard/docs/change-mysql-temp-dir.pdf
    /dashboard/docs/backup-restore-mysql.pdf
    /dashboard/docs/auto-start-xampp.pdf
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

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

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /dashboard/docs/access-phpmyadmin-remotely.pdf
    /dashboard/docs/activate-use-xdebug.pdf
    /dashboard/docs/create-framework-project-zf1.pdf
    /dashboard/docs/create-framework-project-zf2.pdf
    /dashboard/docs/deploy-git-app.pdf
    /dashboard/docs/increase-php-file-upload-limit.pdf
    /dashboard/docs/reset-mysql-password.pdf
    /dashboard/docs/send-mail.pdf
    /dashboard/docs/use-sqlite.pdf
    /dashboard/docs/use-php-fcgi.pdf
    /dashboard/docs/use-different-php-version.pdf
    /dashboard/docs/troubleshoot-apache.pdf
    /dashboard/docs/transfer-files-ftp.pdf
    /dashboard/docs/configure-wildcard-subdomains.pdf
    /dashboard/docs/configure-vhosts.pdf
    /dashboard/docs/configure-use-tomcat.pdf
    /dashboard/docs/change-mysql-temp-dir.pdf
    /dashboard/docs/backup-restore-mysql.pdf
    /dashboard/docs/auto-start-xampp.pdf
```

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: 2025/02/12

Plugin Output

tcp/80/www

```
Webmirror performed 412 queries in 35s (11.0771 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : GET
  Argument :
   Value: mpm_winnt.c


+ CGI : /phpmyadmin/index.php
  Methods : GET,POST
  Argument : DisplayServersList
  Argument : FirstLevelNavigationItems
   Value: 100
  Argument : MaxNavigationItems
   Value: 50
  Argument : NavigationDisplayLogo
  Argument : NavigationDisplayServers
  Argument : NavigationLinkWithMainPanel
  Argument : NavigationLogoLink
   Value: index.php
  Argument : NavigationLogoLinkWindow
  Argument : NavigationTreeAutoexpandSingleDb
  Argument : NavigationTreeDbSeparator
   Value: _
```

```
  Argument : NavigationTreeDefaultTabTable
  Argument : NavigationTreeDefaultTabTable2
  Argument : NavigationTreeDisplayDbFilterMinimum
   Value: 30
  Argument : NavigationTreeDisplayItemFilterMinimum
   Value: 30
  Argument : NavigationTreeEnableExpansion
  Argument : NavigationTreeEnableGrouping
  Argument : NavigationTreePointerEnable
  Argument : NavigationTreeShowEvents
  Argument : NavigationTreeShowFunctions
  Argument : NavigationTreeShowProcedures
  Argument : NavigationTreeShowTables
  Argument : NavigationTreeShowViews
  Argument : NavigationTreeTableLevel
   Value: 1
  Argument : NavigationTreeTableSeparator
   Value: __
  Argument : NavigationWidth
   Value: 240
  Argument : NumFavoriteTables
   Value: 10
  Argument : NumRecentTables
   Value: 10
  Argument : ShowDatabasesNavigationAsTree
  Argument : ajax_request
   Value: 1
  Argument : check_page_refresh
  Argument : collation_connection
  Argument : db
  Argument : favorite_table
   Value: 1
  Argument : lang
  Argument : route
   Value: /license
  Argument : server
   Value: 1
  Argument : set_theme
  Argument : submit_save
   Value: Navi
  Argument : sync_favorite_tables
   Value: 1
  Argument : tab_hash
  Argument : table
  Argument : token
   Value: 697530473a4a6460667852485b59597b
  Argument : viewing_mode
   Value: server


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : url
   Value: [...]
```

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: 2025/02/12

Plugin Output

tcp/443/www

```
Webmirror performed 411 queries in 46s (8.0934 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : GET
  Argument :
   Value: mpm_winnt.c


+ CGI : /phpmyadmin/index.php
  Methods : GET,POST
  Argument : DisplayServersList
  Argument : FirstLevelNavigationItems
   Value: 100
  Argument : MaxNavigationItems
   Value: 50
  Argument : NavigationDisplayLogo
  Argument : NavigationDisplayServers
  Argument : NavigationLinkWithMainPanel
  Argument : NavigationLogoLink
   Value: index.php
  Argument : NavigationLogoLinkWindow
  Argument : NavigationTreeAutoexpandSingleDb
  Argument : NavigationTreeDbSeparator
   Value: _
```

```
  Argument : NavigationTreeDefaultTabTable
  Argument : NavigationTreeDefaultTabTable2
  Argument : NavigationTreeDisplayDbFilterMinimum
   Value: 30
  Argument : NavigationTreeDisplayItemFilterMinimum
   Value: 30
  Argument : NavigationTreeEnableExpansion
  Argument : NavigationTreeEnableGrouping
  Argument : NavigationTreePointerEnable
  Argument : NavigationTreeShowEvents
  Argument : NavigationTreeShowFunctions
  Argument : NavigationTreeShowProcedures
  Argument : NavigationTreeShowTables
  Argument : NavigationTreeShowViews
  Argument : NavigationTreeTableLevel
   Value: 1
  Argument : NavigationTreeTableSeparator
   Value: __
  Argument : NavigationWidth
   Value: 240
  Argument : NumFavoriteTables
   Value: 10
  Argument : NumRecentTables
   Value: 10
  Argument : ShowDatabasesNavigationAsTree
  Argument : ajax_request
   Value: 1
  Argument : check_page_refresh
  Argument : collation_connection
  Argument : db
  Argument : favorite_table
   Value: 1
  Argument : lang
  Argument : route
   Value: /license
  Argument : server
   Value: 1
  Argument : set_theme
  Argument : submit_save
   Value: Navi
  Argument : sync_favorite_tables
   Value: 1
  Argument : tab_hash
  Argument : table
  Argument : token
   Value: 405a4f6e2377276d66572627405d6061
  Argument : viewing_mode
   Value: server


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : url
   Value:  [...]
```

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 : unknown
  URL     : http://192.168.8.250/phpmyadmin/
```

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/443/www

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

  Version : unknown
  URL     : https://192.168.8.250/phpmyadmin/
```