Scan Report

November 18, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.0.4”. The scan started at Fri Nov 18 19:04:01 2022 UTC and ended at Fri Nov 18 19:55:40 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.4	44	62	3	57	0
Total: 1	44	62	3	57	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 166 results selected by the filtering described above. Before filtering there were 166 results.

Host Authentications

Host	Protocol	Result	Port/User
192.168.0.4	SMB	Success	Protocol SMB, Port 445, User

Results per Host

192.168.0.4

Host scan start	Fri Nov 18 19:04:40 2022 UTC
Host scan end	Fri Nov 18 19:55:40 2022 UTC

Service (Port)	Threat Level
443/tcp	High
80/tcp	High
general/tcp	High
445/tcp	High
5900/tcp	Medium
8181/tcp	Medium
25/tcp	Medium
80/tcp	Medium
general/tcp	Medium
80/tcp	Low
general/CPE-T	Log
3306/tcp	Log
5800/tcp	Log
8080/tcp	Log
5900/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
8181/tcp	Log
25/tcp	Log
443/tcp	Log
135/tcp	Log
80/tcp	Log
21/tcp	Log
139/tcp	Log
general/tcp	Log
445/tcp	Log

High 443/tcp

High (CVSS: 10.0)
NVT: Trojan horses

Summary
An unknown service runs on this port. It is sometimes opened by Trojan horses. Unless you know for sure what is behind it, you'd better check your system.

Vulnerability Detection Result

```
An unknown service runs on this port. It is sometimes opened by this/these Troja
↪n horse(s):
 Tabdim
 W32.Kelvir
 Civcat
 W32.Kiman
```

Solution
Solution type: Workaround
If a trojan horse is running, run a good antivirus scanner.

Vulnerability Detection Method
Details: `Trojan horses`
OID:1.3.6.1.4.1.25623.1.0.11157
Version used: `$Revision: 12057 $`

[return to 192.168.0.4]

High 80/tcp

High (CVSS: 7.5)
NVT: Apache HTTP Server Multiple Vulnerabilities June17 (Windows)

... continues on next page ...

. . . continued from previous page . . .

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.26
```

Impact

Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Affected Software/OS

Apache HTTP Server 2.2.x before 2.2.33 and 2.4.x before 2.4.26 on Windows.

Vulnerability Insight

Multiple flaws exists as,

- The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Multiple Vulnerabilities June17 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.811213

Version used: `$Revision: 11863 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2017-7679, CVE-2017-3169, CVE-2017-3167
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:99135, 99134
Other:
  URL:http://seclists.org/oss-sec/2017/q2/509
   URL:http://httpd.apache.org/security/vulnerabilities_24.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:https://httpd.apache.org
```

High (CVSS: 7.5)
NVT: PHP 'libgd' Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.27/7.0.12
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.

Solution

Solution type: VendorFix

Update to PHP version 5.6.27 or 7.0.12.

Affected Software/OS

PHP versions 5.x through 5.6.26 and 7.0.x through 7.0.11 on Windows

Vulnerability Insight

The flaw exists due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'libgd' Denial of Service Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.809337

Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-7568
BID:93184
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
   URL:http://seclists.org/oss-sec/2016/q3/639
   URL:https://bugs.php.net/bug.php?id=73003
```

High (CVSS: 10.0)
NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.43
```

Impact

Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Affected Software/OS

PHP versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Windows

Vulnerability Insight

Multiple flaws are due to

- Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script.

- Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.

Details: `PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (W.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.807092

Version used: `$Revision: 11922 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-5590, CVE-2015-8838, CVE-2015-5589
BID:75970, 88763, 75974
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=69923
```

High (CVSS: 7.5)

NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.45
```

Impact

Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Affected Software/OS

PHP versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807091
Version used: `$Revision: 12363 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-6836
BID:76644
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=70388
```

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.7
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.7 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
PHP versions prior to 5.6.7 on Windows

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'type confusion' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808672
Version used: `$Revision: 12431 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-4601
BID:75246
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP 'var_unserializer' Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.26
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.26, or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
PHP versions prior to 5.6.26 on Windows

Vulnerability Insight
The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'var_unserializer' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809322
Version used: `$Revision: 12338 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-7411
BID:93009
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Arbitrary Code Execution Vulnerability - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to arbitrary code execution vulnerability

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.27
```

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Upgrade to PHP version 5.5.27, or 5.6.11, or later.

Affected Software/OS
PHP versions prior to 5.5.27 and 5.6.x before 5.6.11 on Windows.

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Arbitrary Code Execution Vulnerability - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808670
Version used: `$Revision: 11961 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2015-4116
BID:75127
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 10.0)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)

Product detection result
```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
```
Installed version: 5.4.31
Fixed version:     5.5.32
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.

Affected Software/OS

PHP versions prior to 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 on Windows

Vulnerability Insight

The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808606

Version used: `$Revision: 12363 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-4342, CVE-2016-2554
BID:89154, 83353
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.openwall.com/lists/oss-security/2016/04/28/2
```

High (CVSS: 7.1)

NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.28
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.28, or 5.6.12, or later.

Affected Software/OS

PHP versions prior to 5.5.28 and 5.6.x before 5.6.12 on Windows

Vulnerability Insight

The flaw is due to script 'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Denial of Service Vulnerability - 01 - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808612

Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-8878
BID:90837
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.8)

NVT: PHP Denial of Service Vulnerability Jul17 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     5.6.31
```

Impact

Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of service attack.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Affected Software/OS

PHP versions before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3

Vulnerability Insight

The flaw exists due to improper handling of long form variables in main/php_variables.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service Vulnerability Jul17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811486
Version used: `$Revision: 11874 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2017-11142
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Directory Traversal Vulnerability - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to Directory traversal vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.4.31
Fixed version:     5.4.45
```

Impact

Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.

Affected Software/OS

PHP versions prior to 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Windows

Vulnerability Insight

Multiple flaws are due to

- An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script.
- The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop.
- Improper handling of multiple php_var_unserialize calls.
- Multiple use-after-free vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Directory Traversal Vulnerability - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808616

Version used: `$Revision: 11938 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-9767, CVE-2015-6834, CVE-2015-6835, CVE-2015-6837, CVE-2015-6838
BID:76652, 76649, 76733, 76734, 76738
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.openwall.com/lists/oss-security/2016/03/16/20
```

High (CVSS: 10.0)

NVT: PHP End Of Life Detection (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

The PHP version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "PHP" version on the remote host has reached the end of life.
CPE:               cpe:/a:php:php:5.4.31
Installed version: 5.4.31
EOL version:       5.4
EOL date:          2015-09-03
```

Impact

An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution type: VendorFix

Update the PHP version on the remote host to a still supported version.

Vulnerability Insight

Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.

After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.

Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP End Of Life Detection (Windows)`

OID:1.3.6.1.4.1.25623.1.0.105888

Version used: `$Revision: 12363 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
Other:
  URL:https://secure.php.net/supported-versions.php
   URL:https://secure.php.net/eol.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.30
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (memory consumption or application crash).

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.30, 7.0.15 or later.

Affected Software/OS

PHP versions before 5.6.30 and 7.0.x before 7.0.15

Vulnerability Insight

Multiple flaws are due to

- A integer overflow in the phar_parse_pharfile function in ext/phar/phar.c via a truncated manifest entry in a PHAR archive.

- A off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c via a crafted PHAR archive with an alias mismatch.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.108055

Version used: `$Revision: 11874 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-10159, CVE-2016-10160
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:http://www.php.net/ChangeLog-5.php
 URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Double Free Vulnerabilities - Jan15

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.21/5.6.5
```

Impact

Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.21 or 5.6.5 or later.

Affected Software/OS

PHP versions through 5.5.20 and 5.6.x through 5.6.4

Vulnerability Insight

Multiple flaws are due to:

- Double free error in the 'zend_ts_hash_graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP.
- flaw in the 'GetCode_' function in 'gd_gif_in.c' script in GD Graphics Library (LibGD).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Double Free Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805412
Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2014-9425, CVE-2014-9709
BID:71800, 73306
Other:
  URL:http://securitytracker.com/id/1031479
   URL:https://bugs.php.net/bug.php?id=68676
```

High (CVSS: 7.5)
NVT: PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.31
Fixed Version:     5.4.48
```

Impact

Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Solution

Solution type: VendorFix
Upgrade to PHP 5.4.38 or 5.5.22 or 5.6.6 or later.

Affected Software/OS

PHP versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6

Vulnerability Insight

Multiple flaws are due to,
- Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script.
- Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805689
Version used: `$Revision: 11872 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-0273, CVE-2014-9705
BID:73031, 72701
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1194730
   URL:http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Apr16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.33
```

Impact

Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Solution

Solution type: VendorFix
Upgrade to PHP version 5.5.33 or 5.6.19 or later.

Affected Software/OS

PHP versions before 5.5.33, and 5.6.x before 5.6.19 on Windows

Vulnerability Insight

Multiple flaws are due to,
- A use-after-free error in wddx.c script in the WDDX extension in PHP
- An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Apr16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807806
Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-3142, CVE-2016-3141
Other:
  URL:https://bugs.php.net/bug.php?id=71587
   URL:https://bugs.php.net/bug.php?id=71498
   URL:https://secure.php.net/ChangeLog-5.php
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.37
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

Affected Software/OS

PHP versions prior to 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws are due to,
- The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection.
- The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call.
- The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension.
- The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension.
- An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library.
- An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808787
Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE-2016-5766,
↪CVE-2016-5767
BID:91397, 91398, 91399, 91396, 91395
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Feb15

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     5.4.37
```

Impact

Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Affected Software/OS

PHP versions 5.4.x before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5

Vulnerability Insight

Multiple flaws are due to,

- Flaw in the 'exif_process_unicode' function in ext/exif/exif.c script when parsing JPEG EXIF entries.
- A use-after-free error in the 'process_nested_data' function in ext/standard/var_unserializer.re script.
- a flaw in 'readelf.c' script in Fine Free File.
- an out-of-bounds read flaw in 'src/softmagic.c' script in Fine Free File.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 01 - Feb15`

OID:1.3.6.1.4.1.25623.1.0.805446

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-0232, CVE-2015-0231, CVE-2014-9652, CVE-2014-9653
BID:72505, 72516, 72541, 72539
Other:
  URL:https://bugs.php.net/bug.php?id=68799
   URL:https://bugs.php.net/bug.php?id=68710
```

High (CVSS: 7.5)

NVT: PHP Multiple Vulnerabilities - 01 - Jan15

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.34/5.5.18/5.6.2
```

Impact

Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.34 or 5.5.18 or 5.6.2 or later.

Affected Software/OS

PHP versions 5.4.x before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2

Vulnerability Insight

Multiple flaws are due to,

- The exif_ifd_make_value function in exif.c in the EXIF extension in PHP operates on floating-point arrays incorrectly.
- Integer overflow in the object_custom function in ext/standard/var _unserializer.c in PHP.
- Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxml-rpc/xmlrpc.c in the XMLRPC extension in PHP.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 01 - Jan15`

OID:1.3.6.1.4.1.25623.1.0.805409

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-3670, CVE-2014-3669, CVE-2014-3668
BID:70611, 70665, 70666
Other:
  URL:https://bugs.php.net/bug.php?id=68044
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.34
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.

Affected Software/OS

PHP versions prior to 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 on Windows

Vulnerability Insight

Multiple flaws are due to,

- Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script.
- Format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script.
- An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script.
- An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script.
- An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 01 - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808198

Version used: `$Revision: 12363 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2015-8865
BID:85800, 85801, 85802, 85991, 85993
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jun15 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.31
Fixed Version:     5.4.39
```

Impact

Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Solution

Solution type: VendorFix
Upgrade to PHP 5.4.39 or 5.5.23 or 5.6.7 or later.

Affected Software/OS

PHP versions before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7

Vulnerability Insight

Multiple flaws are due to,
- 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string.
- 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array.
- use-after-free error related to the 'unserialize' function when using DateInterval input.
- a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes.
- an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Jun15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805650
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-4148, CVE-2015-4147, CVE-2015-2787, CVE-2015-2348, CVE-2015-2331
BID:73357, 73431, 73434
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=69085
   URL:http://openwall.com/lists/oss-security/2015/06/01/4
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Mar16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.44
```

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

Affected Software/OS
PHP versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple flaws are due to,
- The multiple use-after-free vulnerabilities in SPL unserialize implementation.
- An insufficient validation of user supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Mar16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807088
Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
BID:76737, 76739, 76735
Other:
  URL:https://bugs.php.net/bug.php?id=70068
   URL:http://www.openwall.com/lists/oss-security/2015/08/19/3
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.37
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to PHP version 5.5.37, or 5.6.23, or later.

Affected Software/OS
PHP versions prior to 5.5.37 and 5.6.x before 5.6.23 on Windows

Vulnerability Insight
Multiple flaws are due to,
- The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection.
- The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 02 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808789
Version used: `$Revision: 12313 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2016-5771, CVE-2016-5770
BID:91401, 91403
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Jan15

Product detection result
```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.4.31
Fixed version:     5.6.5
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.5 or later.

Affected Software/OS
PHP versions before 5.6.5

Vulnerability Insight
The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 02 - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805413
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-9426
Other:
  URL:https://bugs.php.net/bug.php?id=68665
   URL:http://securitytracker.com/id/1031480
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Jun15 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.31
Fixed Version:     5.4.41
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service, bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Solution

Solution type: VendorFix

Upgrade to PHP 5.4.41 or 5.5.25 or 5.6.9 or later.

Affected Software/OS

PHP versions before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9

Vulnerability Insight

Multiple flaws are due to,

- Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP.
- 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character.
- Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP.
- The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 02 - Jun15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805655

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-4026, CVE-2015-4025, CVE-2015-4024, CVE-2015-4022, CVE-2015-4021
BID:75056, 74904, 74903, 74902, 74700
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=69085
   URL:http://openwall.com/lists/oss-security/2015/06/01/4
   URL:http://www.php.net
```

High (CVSS: 7.5)

NVT: PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.25
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later.

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Windows

Vulnerability Insight
Multiple flaws are due to
- An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script.
- An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script.
- An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script.
- Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script.
- Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script.
- Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script.
- The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing.
- Improper handling of certain objects in 'ext/standard/var_unserializer.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809318
Version used: `$Revision: 12051 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128,
↪CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132
BID:92756, 92552, 92755, 92757, 92564, 92758
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.36
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.36, or 5.6.22, or later.

Affected Software/OS

PHP versions prior to 5.5.36 and 5.6.x before 5.6.22 on Windows

Vulnerability Insight

Multiple flaws are due to,

- An integer overflow in the fread function in 'ext/standard/file.c' script.
- An integer overflow in the php_html_entities function in 'ext/standard/html.c' script.
- An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `PHP Multiple Vulnerabilities - 03 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808791
Version used: `$Revision: 14181 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-5096, CVE-2016-5094, CVE-2016-5095
BID:90861, 90857, 92144
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.35
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

Affected Software/OS
PHP versions prior to 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 on Windows.

Vulnerability Insight
The multiple flaws are due to,
- An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script.

. . . continues on next page . . .

. . . continued from previous page . . .

- An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script.
- An improper construction of spprintf arguments, in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script.
- An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'.
- An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script.
- The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures.
- An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script.
- An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 03 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808602
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541,
↪CVE-2016-4542, CVE-2016-4543, CVE-2016-4544
BID:89844, 90172, 90173, 90174
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 10.0)
NVT: PHP Multiple Vulnerabilities - 03 - Jun15 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.31
Fixed Version:     5.4.40
```

. . . continues on next page . . .

... continued from previous page ...

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Solution
Solution type: VendorFix
Upgrade to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Affected Software/OS
PHP versions before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8

Vulnerability Insight
Multiple flaws are due to,
- Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP.
- Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP.
- A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 03 - Jun15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805656
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-3329, CVE-2015-3307, CVE-2015-2783, CVE-2015-1352, CVE-2015-4599,
↪CVE-2015-4600, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE
↪-2015-3411, CVE-2015-3412
BID:74240, 74239, 74703, 75251, 75252, 74413, 75249, 75241, 75233, 75255, 75250
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=69085
   URL:http://openwall.com/lists/oss-security/2015/06/01/4
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Sep16 (Windows)

... continues on next page ...

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.26
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.26, or 7.0.11, or later.

Affected Software/OS

PHP versions prior to 5.6.26 and 7.x before 7.0.11 on Windows

Vulnerability Insight

Multiple flaws are due to,

- Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script.
- Improper varification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script.
- The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough.
- The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type.
- The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library.
- An error in the php_wddx_push_element function in ext/wddx/wddx.c.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 03 - Sep16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.809316

Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417,
↪CVE-2016-7418
BID:93005, 93006, 93004, 93022, 93008, 93007, 93011
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.36
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

Affected Software/OS

PHP versions prior to 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 on Windows

Vulnerability Insight

Multiple flaws are due to,

- The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character.
- The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 04 - Aug16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808793

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2013-7456, CVE-2016-5093
BID:90946, 90859
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.44
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.

Affected Software/OS

PHP versions prior to 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Windows

Vulnerability Insight

The multiple flaws are due to,
- An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script.

. . . continues on next page . . .

. . . continued from previous page . . .

- The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 04 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808605
Version used: `$Revision: 12431 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-8867, CVE-2015-8876, CVE-2015-8873, CVE-2015-8835
BID:87481, 90867, 84426, 90712
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 10.0)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.42
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

PHP versions prior to 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows

Vulnerability Insight

The multiple flaws are due to,
- Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension.
- Integer overflow in the ftp_genlist function in ext/ftp/ftp.c
- PHP does not ensure that pathnames lack %00 sequences.
- An error in 'escapeshellarg' function in 'ext/standard/exec.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808674
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-4644, CVE-2015-4643, CVE-2015-4598, CVE-2015-4642
BID:75291, 75292, 75244, 75290
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.38
```

Impact

Successfully exploiting this issue may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later.

Affected Software/OS

PHP versions before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 on Windows

Vulnerability Insight

Multiple flaws are due to

- An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' script.
- An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi.
- The 'ext/snmp/snmp.c' script improperly interacts with the unserialize implementation and garbage collection.
- The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' script does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function.
- An error in the 'exif_process_user_comment' function in 'ext/exif/exif.c' script.
- An error in the 'exif_process_IFD_in_MAKERNOTE' function in 'ext/exif/exif.c' script.
- The 'ext/session/session.c' does not properly maintain a certain hash data structure.
- An integer overflow in the 'virtual_file_ex' function in 'TSRM/tsrm_virtual_cwd.c' script.
- An error in the 'php_url_parse_ex' function in 'ext/standard/url.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - 05 - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808633

Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292,
↪CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297
BID:92111, 92074, 92097, 92073, 92078, 92115, 92094, 92095, 92099
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://php.net/ChangeLog-7.php
   URL:http://openwall.com/lists/oss-security/2016/07/24/2
   URL:http://www.php.net
```

High (CVSS: 8.5)

NVT: PHP Multiple Vulnerabilities - Dec18 (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.39
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow remote attackers to execute remote code on the affected application/system and/or cause a cause a denial of service.

Solution

Solution type: VendorFix

Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Affected Software/OS

PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.25 and 7.2.x before 7.2.13.

Vulnerability Insight

The flaws exist due to,

- the imap_open functions which allows to run arbitrary shell commands via mailbox parameter.
- a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile.
- ext/standard/var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.
- because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM('WScript.Shell').

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Vulnerabilities - Dec18 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.108508

Version used: `2019-03-29T15:39:23+0000`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2018-19518, CVE-2018-20783, CVE-2018-19395, CVE-2018-19396
BID:106018
Other:
  URL:https://bugs.php.net/bug.php?id=76428
   URL:https://bugs.php.net/bug.php?id=77153
   URL:https://bugs.php.net/bug.php?id=77160
   URL:https://bugs.php.net/bug.php?id=77143
   URL:http://www.securityfocus.com/bid/106018
   URL:https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php
   URL:https://www.exploit-db.com/exploits/45914/
   URL:https://www.openwall.com/lists/oss-security/2018/11/22/3
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Feb19 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.40
Installation
path / port:       80/tcp
```

Solution

Solution type: VendorFix

Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Affected Software/OS

PHP versions before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14 and 7.3.x before 7.3.1.

Vulnerability Insight

PHP is prone to multiple vulnerabilities:

- Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. (CVE-2019-9020)
- A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name. (CVE-2019-9021)
- A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. (CVE-2019-9023)

. . . continues on next page . . .

. . . continued from previous page . . .

- xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas (CVE-2019-9024)

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - Feb19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.142049
Version used: `$Revision: 13857 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024
Other:
  URL:https://bugs.php.net/bug.php?id=77242
   URL:https://bugs.php.net/bug.php?id=77249
   URL:https://bugs.php.net/bug.php?id=77247
   URL:https://bugs.php.net/bug.php?id=77370
   URL:https://bugs.php.net/bug.php?id=77371
   URL:https://bugs.php.net/bug.php?id=77381
   URL:https://bugs.php.net/bug.php?id=77382
   URL:https://bugs.php.net/bug.php?id=77385
   URL:https://bugs.php.net/bug.php?id=77394
   URL:https://bugs.php.net/bug.php?id=77418
   URL:https://bugs.php.net/bug.php?id=77380
```

High (CVSS: 7.5)
NVT: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.37/5.5.21/5.6.5
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Affected Software/OS

PHP versions through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4

Vulnerability Insight

The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Out of Bounds Read Multiple Vulnerabilities - Jan15`

OID:1.3.6.1.4.1.25623.1.0.805414

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-9427
BID:71833
Other:
  URL:https://bugs.php.net/bug.php?id=68618
```

High (CVSS: 7.5)

NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

The host is installed with php and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.34
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution

Solution type: VendorFix

Upgrade to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Affected Software/OS

PHP versions 7.2.x prior to 7.2.3,
PHP versions 7.0.x prior to 7.0.28,
PHP versions 5.0.x prior to 5.6.34 and
PHP versions 7.1.x prior to 7.1.15 on Windows.

Vulnerability Insight

The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812820
Version used: `$Revision: 12391 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2018-7584
BID:103204
Other:
  URL:http://php.net/ChangeLog-7.php
   URL:https://bugs.php.net/bug.php?id=75981
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is installed with PHP and is prone to use-after-free vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.36/5.5.20/5.6.4
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code via a crafted unserialize call.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later.

Affected Software/OS
PHP versions 5.4.x before 5.4.36, 5.5.x before 5.5.20 and 5.6.x before 5.6.4

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the process_nested_data function in ext/standard/var _unserializer.re in PHP.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805411
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-8142
BID:71791
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://secunia.com/advisories/60920
   URL:https://bugs.php.net/bug.php?id=68594
```

High (CVSS: 10.0)
NVT: phpMyAdmin End of Life Detection (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

The phpMyAdmin version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "phpMyAdmin" version on the remote host has reached the end of life.
CPE:               cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Installed version: 4.2.7.1
Location/URL:      http://192.168.0.4/phpmyadmin
EOL version:       4.2
EOL date:          unknown
```

Impact

An end of life version of phpMyAdmin is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution type: VendorFix

Update the phpMyAdmin version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin End of Life Detection (Windows)`

OID:1.3.6.1.4.1.25623.1.0.113030

Version used: `$Revision: 11982 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
Other:
  URL:https://www.phpmyadmin.net/downloads/
   URL:https://www.phpmyadmin.net/news/2011/7/12/phpmyadmin-211-end-of-life/
   URL:https://www.phpmyadmin.net/news/2017/1/23/phpmyadmin-466-441510-and-40101
↪9-are-released/
```

[return to 192.168.0.4]

High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result

```
cpe:/o:microsoft:windows_xp
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "Windows XP" Operating System on the remote host has reached the end of life
↪.
CPE:                   cpe:/o:microsoft:windows_xp
EOL date:              2014-04-08
EOL info:              https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Microsoft%20Windows%20XP&Filter=FilterNO
```

Solution

Solution type: Mitigation

Vulnerability Detection Method

Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `$Revision: 8927 $`

Product Detection Result

Product: `cpe:/o:microsoft:windows_xp`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.0.4]

High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `$Revision: 11874 $`

References

```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

High (CVSS: 10.0)
NVT: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-001.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote unauthenticated attackers to cause denying the service by sending a specially crafted network message to a system running the server service.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 2K Service Pack 4 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.

Vulnerability Insight
The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method
Details: `Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote`
OID:1.3.6.1.4.1.25623.1.0.900233
Version used: `$Revision: 12602 $`

References
```
CVE: CVE-2008-4114, CVE-2008-4834, CVE-2008-4835
BID:31179
Other:
  URL:http://www.milw0rm.com/exploits/6463
   URL:http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx
```

[return to 192.168.0.4]

Medium 5900/tcp

Medium (CVSS: 4.8)
NVT: VNC Server Unencrypted Data Transmission

Summary
The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Vulnerability Detection Result
```
The VNC server provides the following insecure or cryptographically weak Securit
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪y Type(s):
2 (VNC authentication)
```

Impact

An attacker can uncover sensitive data by sniffing traffic to the VNC server.

Solution

Solution type: Mitigation

Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

Vulnerability Detection Method

Details: `VNC Server Unencrypted Data Transmission`

OID:1.3.6.1.4.1.25623.1.0.108529

Version used: `$Revision: 13014 $`

References

```
Other:
  URL:https://tools.ietf.org/html/rfc6143#page-10
```

[return to 192.168.0.4]

Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection

Summary

The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result

```
The following directories with an enabled directory listing were identified:
http://192.168.0.4:8181/
Please review the content manually.
```

Impact

Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution

Solution type: Mitigation

If not needed disable the directory listing within the webservers config.

Affected Software/OS

Webservers with an enabled directory listing.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Check the detected directories if a directory listing is enabled.
Details: `Enabled Directory Listing Detection`
OID:1.3.6.1.4.1.25623.1.0.111074
Version used: `$Revision: 5440 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_
↪Directory_Indexing
```

Medium (CVSS: 5.0)
NVT: Missing ‘httpOnly‘ Cookie Attribute

Summary

The application is missing the ’httpOnly’ cookie attribute

Vulnerability Detection Result

```
The cookies:
Set-Cookie: IDHTTPSESSIONID=***replaced***; path=/
are missing the "httpOnly" attribute.
```

Solution

Solution type: Mitigation
Set the ’httpOnly’ attribute for any session cookie.

Affected Software/OS

Application with session handling in cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the ’httpOnly’ attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method

Check all cookies sent by the application for a missing ’httpOnly’ attribute
Details: `Missing ‘httpOnly‘ Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `$Revision: 5270 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

[return to 192.168.0.4]

Medium 25/tcp

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result

```
'VRFY root' produces the following answer: 550 Address not valid for this site.
```

Solution
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `$Revision: 13470 $`

References

```
Other:
  URL:http://cr.yp.to/smtp/vrfy.html
```

[return to 192.168.0.4]

Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Apache /server-info accessible

Summary
Requesting the URI /server-info gives information about your Apache configuration.

Vulnerability Detection Result

```
Vulnerable url: http://192.168.0.4/server-info
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Requesting the URI /server-info gives information about the currently running Apache.

Solution
Solution type: Workaround
If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.

Affected Software/OS
All Apache versions.

Vulnerability Insight
server-info is a built-in Apache HTTP Server handler used to retrieve the server's status report.

Vulnerability Detection Method
Check if /server-info page exist.
Details: `Apache /server-info accessible`
OID:1.3.6.1.4.1.25623.1.0.10678
Version used: `$Revision: 6411 $`

Medium (CVSS: 5.0)
NVT: Apache /server-status accessible

Summary
Leak of information in Apache.

Vulnerability Detection Result

```
Vulnerable url: http://192.168.0.4/server-status
```

Impact
Requesting the URI /server-status gives information about the currently running Apache.

Solution
If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.

Affected Software/OS
All Apache version.

Vulnerability Insight
server-status is a built-in Apache HTTP Server handler used to retrieve the server's status report.

Vulnerability Detection Method
Check if /server-status page exist.
Details: `Apache /server-status accessible`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.10677
Version used: `$Revision: 6040 $`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone to denial-of-service vulnerability

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.25
```

Impact

Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution

Solution type: VendorFix
Upgrade to Apache HTTP Server 2.4.25 or later.

Affected Software/OS

Apache HTTP Server versions 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2 and 2.4.1 on Windows.

Vulnerability Insight

The flaw exists due to insufficient handling of malicious input to 'mod_auth_digest'.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812066
Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2016-2161
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:95076
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161
```

Medium (CVSS: 6.4)
NVT: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.27
```

Impact

Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Affected Software/OS

Apache HTTP Server 2.2.x before 2.2.34 and 2.4.x before 2.4.27 on Windows.

Vulnerability Insight

The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811236
Version used: `$Revision: 11863 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2017-9788
BID:99569
Other:
  URL:http://www.securitytracker.com/id/1038906
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://httpd.apache.org/security/vulnerabilities_24.html
   URL:https://httpd.apache.org
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.25
```

Impact

Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server 2.2.32 or 2.4.25 or later.

Affected Software/OS

Apache HTTP Server 2.2.x before 2.2.32 and 2.3.x through 2.4.24 prior to 2.4.25

Vulnerability Insight

Multiple flaw exists as application accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.812033
Version used: $Revision: 11983 $

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.10
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2016-8743
BID:95077
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_22.html
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary
The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.30
Installation
path / port:       80/tcp
```

Impact
Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition.

Solution
Solution type: VendorFix
Upgrade to version 2.4.30 or later. For updates refer to reference links.

Affected Software/OS
Apache HTTP server versions 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 through 2.4.18, 2.4.20, 2.4.23, and 2.4.25 through 2.4.29 on Windows.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.812847

Version used: `$Revision: 12116 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2018-1303
BID:103522
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.1)

NVT: Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.24
```

Impact

Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution

Solution type: VendorFix

Upgrade to version 2.4.24, or 2.2.32, or newer.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Apache HTTP Server through 2.4.23 on Windows
- — NOTE: Apache HTTP Server 2.2.32 is not vulnerable
- —

Vulnerability Insight
The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808631
Version used: `$Revision: 12455 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.10`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2016-5387
BID:91816
Other:
  URL:https://www.apache.org/security/asf-httpoxy-response.txt
   URL:http://www.apache.org
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary
This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.13
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension.

Solution
Solution type: VendorFix
Upgrade to version 2.4.13 or later.

Affected Software/OS
Apache HTTP Server versions through 2.4.12.

Vulnerability Insight
Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15`
OID:1.3.6.1.4.1.25623.1.0.805616
Version used: `$Revision: 11975 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.10`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2015-0228
BID:73041
Other:
  URL:https://bugs.mageia.org/show_bug.cgi?id=15428
   URL:http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES
   URL:http://www.apache.org
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability May15

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary
This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 2.4.10
Fixed version:     2.4.12
```

Impact

Successful exploitation will allow a remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution

Solution type: VendorFix

Upgrade to version 2.4.12 or later.

Affected Software/OS

Apache HTTP Server version 2.3.x through 2.4.10.

Vulnerability Insight

Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Mod_Lua Denial of service Vulnerability May15`

OID:1.3.6.1.4.1.25623.1.0.805637

Version used: `$Revision: 11975 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2014-8109
BID:73040
Other:
  URL:http://httpd.apache.org/security/vulnerabilities_24.html
   URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109
   URL:http://www.apache.org
```

Medium (CVSS: 5.0)

NVT: Apache HTTP Server Mod_Proxi_Fcgi Denial of service Vulnerability May15

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.12
```

Impact

Successful exploitation will allow a remote attackers to cause a denial of service via specially crafted response.

Solution

Solution type: VendorFix

Upgrade to version 2.4.12 or later.

Affected Software/OS

Apache HTTP Server version 2.4.10.

Vulnerability Insight

Flaw is due to an out-of-bounds read condition in the 'handle_headers' function in mod_proxy_fcgi that is triggered as user-supplied input is not properly validated when handling responses from FastCGI servers.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Mod_Proxi_Fcgi Denial of service Vulnerability May15`

OID:1.3.6.1.4.1.25623.1.0.805636

Version used: `$Revision: 11975 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2014-3583
BID:71657
Other:
  URL:https://bugzilla.redhat.com/show_bug.cgi?id=1163555
    URL:http://httpd.apache.org/security/vulnerabilities_24.html
    URL:http://www.apache.org
```

Medium (CVSS: 6.8)

NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

The host is installed with Apache HTTP server and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.30
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution

Solution type: VendorFix

Upgrade to version 2.4.30 or later. For updates refer to reference links.

Affected Software/OS

Apache HTTP server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29 on Windows.

Vulnerability Insight

Multiple flaws exists due to,

- Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks.
- Misconfigured mod_session variable, HTTP_SESSION.
- Apache HTTP Server fails to sanitize the expression specified in '<FilesMatch>'.
- An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig.
- Apache HTTP Server fails to sanitize against a specially crafted request.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.812846

Version used: `$Revision: 12068 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301
BID:103524, 103520, 103525, 103512, 103515
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Multiple Vulnerabilities August15 (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.14
```

Impact

Successful exploitation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution

Solution type: VendorFix

Upgrade to version 2.4.14 or later.

Affected Software/OS

Apache HTTP Server version 2.4.x before 2.4.14 on windows.

Vulnerability Insight

Multiple flaws are due to:

- an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting.
- an error in chunked transfer coding implementation.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server Multiple Vulnerabilities August15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805698

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.10`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2015-3185, CVE-2015-3183
BID:75965, 75963
Other:
  URL:http://www.apache.org/dist/httpd/CHANGES_2.4
   URL:http://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed)

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary
Apache HTTP server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.28
```

Impact
The successful exploitation allows the attacker to read chunks of the host's memory.

Solution
Solution type: VendorFix
Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references.
As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods.

Affected Software/OS
Apache HTTP Server 2.2.x versions up to 2.2.34 and 2.4.x below 2.4.28.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Optionsbleed is a use after free error in Apache HTTP server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked.

The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method.

Example .htaccess:

<Limit abcxyz> </Limit>

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed)`

OID:1.3.6.1.4.1.25623.1.0.108252

Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2017-9798
BID:100872
Other:
  URL:http://openwall.com/lists/oss-security/2017/09/18/2
   URL:https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-
↪leak-Apaches-server-memory.html
   URL:http://www.securityfocus.com/bid/100872
   URL:https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/
   URL:https://www.apache.org/dist/httpd/CHANGES_2.4.28
```

Medium (CVSS: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary

Debugging functions are enabled on the remote web server.

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

Vulnerability Detection Result

```
The web server has the following HTTP methods enabled: TRACE
```

Impact

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method

Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 10828 $`

References

```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683,
↪CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE
↪-2014-7883
BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     1.9.0
```

Solution

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `$Revision: 12183 $`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.8.3`

Method: `jQuery Detection`

OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
CVE: CVE-2012-6708
Other:
  URL:https://bugs.jquery.com/ticket/11290
```

Medium (CVSS: 4.3)

NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.8.3
Fixed version:     1.9.0
```

Solution
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `$Revision: 12183 $`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.8.3`
Method: `jQuery Detection`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References
```
CVE: CVE-2012-6708
Other:
  URL:https://bugs.jquery.com/ticket/11290
```

Medium (CVSS: 4.3)
NVT: jQuery < 3.0.0 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerability Detection Result
```
Installed version: 1.8.3
Fixed version:     3.0.0
```

Solution
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 3.0.0 or later or apply the patch.

Affected Software/OS
jQuery prior to version 3.0.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 3.0.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141635
Version used: `$Revision: 12183 $`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.8.3`
Method: `jQuery Detection`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
CVE: CVE-2015-9251
Other:
  URL:https://github.com/jquery/jquery/issues/2432
```

Medium (CVSS: 4.3)
NVT: jQuery < 3.0.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.8.3
Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     3.0.0
```

Solution
Solution type: VendorFix
Update to version 3.0.0 or later or apply the patch.

Affected Software/OS
jQuery prior to version 3.0.0.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `jQuery < 3.0.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141635

Version used: `$Revision: 12183 $`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.8.3`

Method: `jQuery Detection`

OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
CVE: CVE-2015-9251
Other:
  URL:https://github.com/jquery/jquery/issues/2432
```

Medium (CVSS: 5.0)

NVT: PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to a Denial of Service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.39
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow attackers to cause a denial of service of the affected application.

Solution

Solution type: VendorFix

Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Affected Software/OS

PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.26 and 7.2.x before 7.2.14.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw exist due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.108506

Version used: `$Revision: 12938 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2018-19935
BID:106143
Other:
  URL:https://bugs.php.net/bug.php?id=77020
   URL:http://www.securityfocus.com/bid/106143
```

Medium (CVSS: 5.0)

NVT: PHP 'donate' function Denial of Service Vulnerability - Nov14

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.35/5.5.19/5.6.3
```

Impact

Successful exploitation will allow a local attacker to conduct a denial of service attack.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.35 or 5.5.19 or 5.6.3 or later.

Affected Software/OS

PHP versions 5.4.x before 5.4.35, 5.5.x before 5.5.19 and 5.6.x before 5.6.3

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw is due to an out-of-bounds read error in the 'donote' function in readelf.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'donate' function Denial of Service Vulnerability - Nov14`
OID:1.3.6.1.4.1.25623.1.0.804884
Version used: `$Revision: 11867 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-3710
BID:70807
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=68283
   URL:http://xforce.iss.net/xforce/xfdb/98385
```

Medium (CVSS: 5.0)
NVT: PHP 'gdImageScaleTwoPass()' Multiple Denial of Service Vulnerabilities (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.12
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consuption).

Solution

Solution type: VendorFix
Upgrade to PHP version 5.6.12 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
PHP versions prior to 5.6.12 on Windows

Vulnerability Insight
Multiple flaws are due to
- An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script.
- The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'gdImageScaleTwoPass()' Multiple Denial of Service Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808610
Version used: `$Revision: 11903 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-8877, CVE-2015-8879, CVE-2015-8874
BID:90866, 90842, 90714
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 6.4)
NVT: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.44
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or 7.0.4, or later.

Affected Software/OS

PHP versions prior to 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 on Windows

Vulnerability Insight

The flaw is due an error in the 'make_http_soap_request' function in 'ext/soap/php_http.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'make_http_soap_request' Information Disclosure Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808667

Version used: `$Revision: 12338 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-3185
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 4.3)

NVT: PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to cross site scripting and denial of service vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.4.31
Fixed version:     5.6.33
Installation
path / port:       80/tcp
```

Impact

Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Affected Software/OS

PHP versions before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1

Vulnerability Insight

Multiple flaws are due to,

- An input validation error on the PHAR 404 error page via the URI of a request for a .phar file.
- An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)`

OID:1.3.6.1.4.1.25623.1.0.812732

Version used: `$Revision: 12120 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2018-5712, CVE-2018-5711
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://php.net/ChangeLog-7.php
   URL:https://bugs.php.net/bug.php?id=74782
   URL:https://bugs.php.net/bug.php?id=75571
   URL:http://www.php.net
```

Medium (CVSS: 6.4)

NVT: PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.30
```

Impact

Successfully exploiting this issue allow remote attackers to supply malicious archive files to crash the PHP interpreter or potentially disclose information.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.30 or 7.0.15, or later.

Affected Software/OS

PHP versions before 5.6.30, 7.x before 7.0.15

Vulnerability Insight

The flaw exists due to a buffer over-read error in the 'phar_parse_pharfile' function in ext/phar/phar.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Windows)`

OID:1.3.6.1.4.1.25623.1.0.811483

Version used: `$Revision: 11982 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2017-11147
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 6.8)
NVT: PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     7.1.20
Installation
path / port:       80/tcp
```

Impact

Successfully exploitation will allow an attackers to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Solution

Solution type: VendorFix

Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Affected Software/OS

PHP versions 5.x up to and including 5.6.36. All 7.0.x versions, 7.1.x before 7.1.20, 7.2.x before 7.2.8 and 7.3.x before 7.3.0alpha3 on Windows.

Vulnerability Insight

The flaw exist due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812519
Version used: `$Revision: 12762 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-9253
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:https://bugs.php.net/bug.php?id=73342
   URL:https://bugs.php.net/bug.php?id=70185
   URL:https://github.com/php/php-src/pull/3287
   URL:https://www.futureweb.at/security/CVE-2015-9253
   URL:https://vuldb.com//?id.113566
```

Medium (CVSS: 5.0)
NVT: PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.32
Installation
path / port:       80/tcp
```

Impact

Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and availability.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Affected Software/OS

PHP versions before 5.5.32, 7.0.x before 7.0.3, and 5.6.x before 5.6.18 on Windows.

Vulnerability Insight

The flaw exists due to error in the function stream_get_meta_data of the component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metadata).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.812513

Version used: `$Revision: 12120 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-10712
Other:
  URL:https://vuldb.com/?id.113055
   URL:https://bugs.php.net/bug.php?id=71323
   URL:https://git.php.net/?p=php-src.git;a=commit;h=6297a117d77fa3a0df2e21ca926
↪a92c231819cd5
   URL:http://www.php.net
```

Medium (CVSS: 5.0)
NVT: PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to heap buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.32
Installation
path / port:       80/tcp
```

Impact

Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Affected Software/OS

PHP versions before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11

Vulnerability Insight

The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.812072

Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2017-16642
BID:101745
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://php.net/ChangeLog-7.php
   URL:https://bugs.php.net/bug.php?id=75055
   URL:http://www.php.net
```

Medium (CVSS: 5.0)
NVT: PHP 'URL checks' Security Bypass Vulnerability Jul17 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.28
```

Impact

Successfully exploiting this issue allow an attacker to bypass hostname-specific URL checks.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.28, 7.0.13, or later.

Affected Software/OS

PHP versions before 5.6.28, 7.x before 7.0.13

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight

The flaw exists due to incorrect handling of various URI components in the URL parser.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'URL checks' Security Bypass Vulnerability Jul17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811488
Version used: `$Revision: 11959 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-10397
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 5.0)
NVT: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.31
```

Impact

Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.6.31 or later.

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

PHP versions before 5.6.31.

Vulnerability Insight

The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811485
Version used: `$Revision: 11959 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2017-11143
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 4.3)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.38
```

Impact

Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

PHP versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 on Windows

Vulnerability Insight

The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Cross-Site Scripting Vulnerability - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808799
Version used: `$Revision: 12149 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-8935
BID:92356
Other:
  URL:https://bugs.php.net/bug.php?id=68978
   URL:http://www.php.net
```

Medium (CVSS: 6.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.18
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.18, or 7.0.3, or later.

Affected Software/OS

PHP versions prior to 5.6.18 and 7.x before 7.0.3 on Windows

Vulnerability Insight

The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808608

Version used: `$Revision: 11903 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-4343
BID:89179
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.openwall.com/lists/oss-security/2016/04/28/2
```

Medium (CVSS: 6.4)

NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.31
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Windows.

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service Vulnerability - 02 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809138
Version used: `$Revision: 12096 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-5114
BID:81808
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 5.0)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.0

Affected Software/OS
PHP versions prior to 5.6.0 on Windows

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Fileinfo Component Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808668
Version used: `$Revision: 11903 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2014-0236
BID:90957
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 5.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Windows)

Product detection result
```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.

Vulnerability Detection Result
```
Installed version: 5.4.31
Fixed version:     5.6.24/7.0.9
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.

Solution

Solution type: VendorFix

Update to PHP version 5.6.24 or 7.0.19.

Affected Software/OS

PHP versions 5.x through 5.6.23 and 7.0.x through 7.0.8 on Windows

Vulnerability Insight

The following flaws exist:

- The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables.
- 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications
- An unspecified flaw in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808627

Version used: `$Revision: 11969 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-5385, CVE-2016-6128
BID:91821, 91509
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.kb.cert.org/vuls/id/797896
   URL:https://bugs.php.net/bug.php?id=72573
   URL:https://bugs.php.net/bug.php?id=72494
```

Medium (CVSS: 6.8)

NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Windows)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result

```
Installed Version: 5.4.31
Fixed Version:     5.5.30
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).

Solution

Solution type: VendorFix

Upgrade to PHP 5.5.30 or 5.6.14 or later.

Affected Software/OS

PHP versions before 5.5.30 and 5.6.x before 5.6.14

Vulnerability Insight

Multiple flaws are due to,

- An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script.
- An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.806648

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-7804, CVE-2015-7803
BID:76959
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=70433
   URL:http://www.openwall.com/lists/oss-security/2015/10/05/8
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.30
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer over-read or application crash).

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.30, 7.0.15, 7.1.1 or later.

Affected Software/OS

PHP versions before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1.

Vulnerability Insight

Multiple flaws are due to

- The exif_convert_any_to_int function in ext/exif/exif.c tries to divide the minimum representable negative integer by -1.
- A mishandled serialized data in a finish_nested_data call within the object_common1 function in ext/standard/var_unserializer.c.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.108053

Version used: `$Revision: 11874 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-10161, CVE-2016-10158
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:http://www.php.net/ChangeLog-5.php
 URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple heap buffer overflow and information disclosure vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.37
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. For updates refer to Reference links.

Affected Software/OS

PHP versions before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8

Vulnerability Insight

Multiple flaws exist due to,

- exif_process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files.
- exif_thumbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageInfo->Thumbnail.size'
- linkinfo function on windows doesn't implement openbasedir check.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (W.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.813597

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 12120 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2018-14851, CVE-2018-14883, CVE-2018-15132
Other:
  URL:https://access.redhat.com/security/cve/cve-2018-14851
   URL:http://www.php.net
   URL:https://bugs.php.net/bug.php?id=76557
   URL:https://bugs.php.net/bug.php?id=76423
   URL:https://bugs.php.net/bug.php?id=76459
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities - 01 - Aug14

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.32/5.5.16
```

Impact
Successful exploitation will allow remote attackers to overwrite arbitrary files, conduct denial of service attacks or potentially execute arbitrary code.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.32 or 5.5.16 or later.

Affected Software/OS
PHP version 5.4.x before 5.4.32 and 5.5.x before 5.5.16

Vulnerability Insight
The flaws exist due to,
- Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script.

. . . continues on next page . . .

. . . continued from previous page . . .

- Integer overflow in the 'cdf_read_property_info' function in cdf.c within the Fileinfo component.
- An error in the '_php_image_output_ctx' function within ext/gd/gd_ctx.c script as NULL bytes in paths to various image handling functions are not stripped.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Aug14`
OID:1.3.6.1.4.1.25623.1.0.804820
Version used: `$Revision: 11867 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-3597, CVE-2014-3587, CVE-2014-5120
BID:69322, 69325, 69375
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://secunia.com/advisories/59709
   URL:http://secunia.com/advisories/57349
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities - 04 - Jun15 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.4.40
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly execute arbitrary code via pipelined HTTP requests.

Solution
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Affected Software/OS

PHP versions before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8

Vulnerability Insight

The flaw is due to vulnerability in 'php_handler' function in sapi/apache2handler/sapi_apache2.c script in PHP.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 04 - Jun15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805659
Version used: `$Revision: 12986 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-3330
BID:74204
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=69085
   URL:http://openwall.com/lists/oss-security/2015/06/01/4
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Vulnerabilities - Jul17 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.31
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.31, 7.0.21, 7.1.7, or later.

Affected Software/OS
PHP versions before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7

Vulnerability Insight
Multiple flaws are due to
- An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function.
- The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function.
- lack of bounds checks in the date extension's timelib_meridian parsing code.
- A stack-based buffer overflow in the zend_ini_do_op() function in 'Zend/zend_ini_parser.c' script.
- The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - Jul17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811481
Version used: `$Revision: 11863 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2017-11145, CVE-2017-11144, CVE-2017-11146, CVE-2017-11628, CVE-2017-78
↪90
BID:99492, 99550, 99605, 99612, 99489
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities May18 (Windows)

Product detection result
```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
The host is installed with php and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.36
Installation
path / port:       80/tcp
```

Impact
Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution
Solution type: VendorFix
Upgrade to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. For updates refer to Reference links.

Affected Software/OS
PHP versions prior to 5.6.36,
PHP versions 7.2.x prior to 7.2.5,
PHP versions 7.0.x prior to 7.0.30,
PHP versions 7.1.x prior to 7.1.17 on Windows.

Vulnerability Insight
Multiple flaws exists due to
- An out of bounds read error in 'exif_read_data' function while processing crafted JPG data.
- An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence.
- An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP.
- An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities May18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813159
Version used: `$Revision: 12120 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2018-10549, CVE-2018-10546, CVE-2018-10548, CVE-2018-10547
Other:
  URL:http://www.php.net/ChangeLog-5.php#5.6.36
   URL:http://www.php.net/ChangeLog-7.php#7.0.30
   URL:http://www.php.net/ChangeLog-7.php#7.1.17
   URL:http://www.php.net/ChangeLog-7.php#7.2.5
```

Medium (CVSS: 6.4)
NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.31
```

Impact

Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Affected Software/OS

PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Windows

Vulnerability Insight

The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.807089

Version used: `$Revision: 11961 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2016-1903
BID:79916
Other:
  URL:https://bugs.php.net/bug.php?id=70976
   URL:http://www.openwall.com/lists/oss-security/2016/01/14/8
   URL:http://www.php.net
```

Medium (CVSS: 6.8)
NVT: PHP Sessions Subsystem Session Fixation Vulnerability - Aug13 (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is running PHP and is prone to session fixation vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.2
```

Impact
Successful exploitation will allow attackers to hijack web sessions by specifying a session ID.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.2 or later.

Affected Software/OS
PHP version prior to 5.5.2 on Windows.

Vulnerability Insight
PHP contains an unspecified flaw in the Sessions subsystem.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Sessions Subsystem Session Fixation Vulnerability - Aug13 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803737

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 11865 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2011-4718
Other:
  URL:http://secunia.com/advisories/54562
   URL:http://cxsecurity.com/cveshow/CVE-2011-4718
   URL:http://git.php.net/?p=php-src.git;a=commit;h=169b78eb79b0e080b67f9798708e
↪b3771c6d0b2f
   URL:http://git.php.net/?p=php-src.git;a=commit;h=25e8fcc88fa20dc9d4c471844710
↪03f436927cde
   URL:http://php.net
```

Medium (CVSS: 6.8)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Windows)

Product detection result

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerabilities

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.5.22
```

Impact
Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.22, or 5.6.6, or later.

Affected Software/OS
PHP versions prior to 5.5.22 and 5.6.x before 5.6.6 on Windows

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP XML Entity Expansion And XML External Entity Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808614
Version used: `$Revision: 14181 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-8866
BID:87470
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'CVE-2014-6300' Cross-Site Scripting (XSS) Vulnerability (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.8.1
```

Solution
Solution type: VendorFix
Update to version 4.2.8.1, 4.1.14.4 or 4.0.10.3.

Affected Software/OS
phpMyAdmin 4.2.x before 4.2.8.1, 4.1.x before 4.1.14.4 and 4.0.x before 4.0.10.3

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `phpMyAdmin 'CVE-2014-6300' Cross-Site Scripting (XSS) Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.112018
Version used: `$Revision: 12106 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2014-6300
BID:69790
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2014-10/
```

Medium (CVSS: 5.0)
NVT: phpMyAdmin 'libraries/select_lang.lib.php' Information-Disclosure Vulnerability March15

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
This host is installed with phpMyAdmin and is prone to an information-disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.13.2
```

Impact
Successfully exploiting this issue makes it easier for remote attackers to conduct a BREACH attack and determine this token via a series of crafted requests.

Solution
Solution type: VendorFix
Upgrade to phpMyAdmin 4.0.10.9 or newer, or 4.2.13.2 or newer, or 4.3.11.1 or newer.

Affected Software/OS
phpMyAdmin versions 4.0.x before 4.0.10.9, 4.2.x before 4.2.13.2, and 4.3.x before 4.3.11.1

Vulnerability Insight
libraries/select_lang.lib.php includes invalid language values in unknown-language error responses that contain a CSRF token and may be sent with HTTP compression

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin 'libraries/select_lang.lib.php' Information-Disclosure Vulnerability.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.111075
Version used: `$Revision: 12363 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2015-2206
BID:72949
Other:
  URL:http://www.securityfocus.com/bid/72949
   URL:https://www.phpmyadmin.net/security/PMASA-2015-1/
   URL:http://www.phpmyadmin.net
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin 4.0 <= 4.8.4 Arbitrary File Read Vulnerability - PMASA-2019-1 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to an arbitrary file read vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.8.5
Installation
path / port:       /phpmyadmin
```

Solution
Solution type: VendorFix
Update to version 4.8.5.

Affected Software/OS
phpMyAdmin versions 4.0 through 4.8.4.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

When AllowArbitraryServer configuration set to true, with the use of a rogue MySQL server, an attacker can read any file on the server that the web server's user can access.
phpMyadmin attempts to block the use of LOAD DATA INFILE, but due to a bug in PHP, this check is not honored. Additionally, when using the 'mysql' extension, mysql.allow_local_infile is enabled by default. Both of these conditions allow the attack to occur.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin 4.0 <= 4.8.4 Arbitrary File Read Vulnerability - PMASA-2019-1 (Windo.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.112501
Version used: `$Revision: 13374 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2019-6799
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2019-1/
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin 4.x < 4.8.4 Multiple Vulnerabilities - PMASA-2018-6, PMASA-2018-8 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.8.4
Installation
path / port:       /phpmyadmin
```

Solution
Solution type: VendorFix
Update to version 4.8.4 or later.

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

phpMyAdmin versions from at least 4.0 through 4.8.3.

Vulnerability Insight

- A flaw has been found where an attacker can exploit phpMyAdmin to leak the contents of a local file. The attacker must have access to the phpMyAdmin Configuration Storage tables, although these can easily be created in any database to which the attacker has access. An attacker must have valid credentials to log in to phpMyAdmin. This vulnerability does not allow an attacker to circumvent the login system (CVE-2018-19968).

- A Cross-Site Scripting vulnerability was found in the navigation tree, where an attacker can deliver a payload to a user through a specially-crafted database/table name (CVE-2018-19970).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin 4.x < 4.8.4 Multiple Vulnerabilities - PMASA-2018-6, PMASA-2018-8 (W.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.108514

Version used: `$Revision: 12954 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2018-19968, CVE-2018-19970
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2018-6/
   URL:https://www.phpmyadmin.net/security/PMASA-2018-8/
```

Medium (CVSS: 4.3)

NVT: phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

phpMyAdmin is prone to an authenticated Cross-Site Scripting (XSS) Vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.8.3
```

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 4.8.3.

Affected Software/OS

phpMyAdmin through version 4.8.2.

Vulnerability Insight

An authenticated attacker could trick a user into importing a specially crafted file, resulting in the attacker gaining control over the user's account.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.113256
Version used: `$Revision: 12164 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2018-15605
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2018-5/
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Windows

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

This host is installed with phpMyAdmin and is prone to cross site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.8.2
Installation
path / port:       /phpmyadmin
```

Impact

Successful exploitation will allow an attacker to inject arbitrary web script or HTML via crafted database name.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade to version 4.8.2 or newer. For updates refer to Reference links.

Affected Software/OS
phpMyAdmin versions prior to 4.8.2 on windows

Vulnerability Insight
The flaw exists due to insufficient validation of input passed to 'js/designer/move.js' script in phpMyAdmin.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Windows`
OID:1.3.6.1.4.1.25623.1.0.813450
Version used: `$Revision: 12025 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2018-12581
BID:104530
Other:
  URL:https://www.phpmyadmin.net
   URL:https://www.phpmyadmin.net/security/PMASA-2018-3
```

Medium (CVSS: 5.0)
NVT: phpMyAdmin Denial-of-Service Vulnerability -01 Dec14

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
This host is installed with phpMyAdmin and is prone to denial-of-service vulnerability.

Vulnerability Detection Result
```
Installed version: 4.2.7.1
Fixed version:     4.2.13.1
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to cause the affected application to crash, denying service to legitimate users.

Solution

Solution type: VendorFix

Upgrade to phpMyAdmin 4.0.10.7 or 4.1.14.8 or 4.2.13.1 or later.

Affected Software/OS

phpMyAdmin versions 4.0.x prior to 4.0.10.7, 4.1.x prior to 4.1.14.8 and 4.2.x prior to 4.2.13.1

Vulnerability Insight

The flaw exists due to an error triggered during the handling of long passwords

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin Denial-of-Service Vulnerability -01 Dec14`

OID:1.3.6.1.4.1.25623.1.0.805307

Version used: `$Revision: 11974 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2014-9218
BID:71434
Other:
  URL:http://1337day.com/exploit/23007
   URL:http://secunia.com/advisories/60454
   URL:http://xforce.iss.net/xforce/xfdb/99140
   URL:http://www.phpmyadmin.net/home_page/security/PMASA-2014-17.php
```

Medium (CVSS: 5.0)

NVT: phpMyAdmin Information Disclosure Vulnerability

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

This host is installed with phpMyAdmin and is prone to information disclosure vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable url: http://192.168.0.4/phpmyadmin/libraries/config/messages.inc.php
```

Impact

Successful exploitation will allow remote attackers to obtain sensitive information about the server.

Solution

Solution type: VendorFix

Upgrade to phpMyAdmin version 4.0.10.12 or 4.4.15.2 or 4.5.3.1 or later or apply patch from the link mentioned in reference.

Affected Software/OS

phpMyAdmin versions 4.0.x prior to 4.0.10.12, 4.4.x prior to 4.4.15.2 and 4.5.x prior to 4.5.3.1

Vulnerability Insight

The flaw is due to recommended setting of the PHP configuration directive display_errors is set to on, which is against the recommendations given in the PHP manual for a production server.

Vulnerability Detection Method

Send a crafted request via HTTP GET and check whether it is able to obtain sensitive information or not.

Details: `phpMyAdmin Information Disclosure Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.807055

Version used: `$Revision: 11811 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2015-8669
BID:79691
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2015-6
   URL:https://github.com/phpmyadmin/phpmyadmin/commit/c4d649325b25139d7c097e56e
↪2e46cc7187fae45
   URL:https://www.phpmyadmin.net
```

Medium (CVSS: 6.5)
NVT: phpMyAdmin Multiple Vulnerabilities - 30-Nov-14 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
phpMyAdmin is prone to multiple cross-site scripting (XSS) and directory traversal vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.2.7.1
Fixed version:     4.2.12
```

Solution
Solution type: VendorFix
Update to version 4.0.10.6, 4.1.14.7 or 4.2.12.

Affected Software/OS
phpMyAdmin 4.0.x before 4.0.10.6, 4.1.x before 4.1.14.7 and 4.2.x before 4.2.12

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin Multiple Vulnerabilities - 30-Nov-14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.112001
Version used: `$Revision: 12106 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2014-8958, CVE-2014-8959
BID:71247, 71243
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2014-13/
   URL:https://www.phpmyadmin.net/security/PMASA-2014-14/
```

Medium (CVSS: 4.0)
NVT: phpMyAdmin Multiple Vulnerabilities - 30-Nov-14 (Windows) (02)

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

phpMyAdmin is prone to multiple cross-site scripting (XSS) and directory traversal vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.12
```

Solution

Solution type: VendorFix

Update to version 4.1.14.7 or 4.2.12.

Affected Software/OS

phpMyAdmin 4.1.x before 4.1.14.7 and 4.2.x before 4.2.12

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin Multiple Vulnerabilities - 30-Nov-14 (Windows) (02)`

OID:1.3.6.1.4.1.25623.1.0.112003

Version used: `$Revision: 12106 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2014-8960, CVE-2014-8961
BID:71244, 71245
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2014-15/
   URL:https://www.phpmyadmin.net/security/PMASA-2014-16/
```

Medium (CVSS: 5.0)

NVT: phpMyAdmin Multiple Vulnerabilities -01 Feb16

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

This host is installed with phpMyAdmin and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Vulnerable url: http://192.168.0.4/phpmyadmin/setup/lib/common.inc.php
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow remote attackers to obtain sensitive information about the server and to inject arbitrary web script or HTML, to bypass intended access restrictions and to guess passwords.

Solution
Solution type: VendorFix
Upgrade to phpMyAdmin version 4.0.10.13 or 4.4.15.3 or 4.5.4 or later or apply patch from the link mentioned in reference.

Affected Software/OS
phpMyAdmin versions 4.0.x prior to 4.0.10.13, 4.4.x prior to 4.4.15.3 and 4.5.x prior to 4.5.4

Vulnerability Insight
Multiple flaws are due to,
- The recommended setting of the PHP configuration directive display_errors is set to on, which is against the recommendations given in the PHP manual for a production server.
- The XSRF/CSRF token is generated with a weak algorithm using functions that do not return cryptographically secure values.
- An insufficient validation of user supplied input via parameters table name, SET value, hostname header and search query.
- The password suggestion functionality uses 'Math.random' function which does not provide cryptographically secure random numbers.
- The 'libraries/common.inc.php' script does not use a constant-time algorithm for comparing CSRF tokens.

Vulnerability Detection Method
Send a crafted request via HTTP GET and check whether it is able to obtain sensitive information or not.
Details: `phpMyAdmin Multiple Vulnerabilities -01 Feb16`
OID:1.3.6.1.4.1.25623.1.0.807080
Version used: `$Revision: 12149 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2016-2038, CVE-2016-2039, CVE-2016-2040, CVE-2016-2041, CVE-2016-1927
BID:82075, 81210, 82077, 82084, 82076
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2016-4
   URL:https://www.phpmyadmin.net/security/PMASA-2016-5
   URL:https://www.phpmyadmin.net/security/PMASA-2016-3
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:https://www.phpmyadmin.net/security/PMASA-2016-2
URL:https://www.phpmyadmin.net/security/PMASA-2016-1
```

Medium (CVSS: 6.8)
NVT: phpMyAdmin Multiple Vulnerabilities -01 June15

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

This host is installed with phpMyAdmin and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.13.3
```

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack or by conducting a cross-site scripting attacks, Web cache poisoning, and other malicious activities.

Solution

Solution type: VendorFix

Upgrade to phpMyAdmin 4.0.10.10, or 4.2.13.3 or 4.3.13.1 or 4.4.6.1 or later.

Affected Software/OS

phpMyAdmin versions 4.0.x before 4.0.10.10, 4.2.x before 4.2.13.3, 4.3.x before 4.3.13.1, and 4.4.x before 4.4.6.1

Vulnerability Insight

Multiple flaws are due to,

- 'libraries/Config.class.php' disables X.509 certificate verification for GitHub API calls over SSL
- HTTP requests do not require multiple steps, explicit confirmation, or a unique token when performing certain sensitive actions.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin Multiple Vulnerabilities -01 June15`

OID:1.3.6.1.4.1.25623.1.0.805398

Version used: `$Revision: 11975 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2015-3902, CVE-2015-3903
BID:74660, 74657
Other:
  URL:http://www.securitytracker.com/id/1032404
   URL:http://www.phpmyadmin.net/home_page/security/PMASA-2015-2.php
```

Medium (CVSS: 5.0)
NVT: Unprotected Web App Installers (HTTP)

Summary
The script attempts to identify installation pages of various Web Apps that are publicly accessible and not protected by account restrictions.

Vulnerability Detection Result

```
The following Web App installers are unprotected and publicly accessible  (URL:D
↪escription):
http://192.168.0.4/phpmyadmin/setup/index.php:CubeCart / phpMyAdmin installer
```

Impact
It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

Solution
Solution type: Mitigation
Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Detection Method
Enumerate the remote web server and check if unprotected Web Apps are accessible for installation.
Details: `Unprotected Web App Installers (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107307
Version used: `$Revision: 12754 $`

[return to 192.168.0.4]

Medium general/tcp

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:apache:http_server:2.4.10
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Vulnerability Detection Result

```
Installed version: 2.4.10
Fixed version:     2.4.38
```

Solution

Solution type: VendorFix

Update to version 2.4.38 or later.

Affected Software/OS

Apache HTTP server version 2.4.37 and prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.141963

Version used: `$Revision: 13750 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.10`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2018-17199
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

[return to 192.168.0.4]

Low 80/tcp

Low (CVSS: 1.9)
NVT: PHP Security Bypass Vulnerability May18 (Windows)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:php:php:5.4.31
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
The host is installed with php and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.31
Fixed version:     5.6.35
Installation
path / port:       80/tcp
```

Impact
Successful exploitation will allow an attacker to bypass security restrictions and access sensitive configuration data for other accounts directly in the PHP worker process's memory.

Solution
Solution type: VendorFix
Upgrade to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. For updates refer to Reference links.

Affected Software/OS
PHP versions prior to 5.6.35,
PHP versions 7.2.x prior to 7.2.4,
PHP versions 7.0.x prior to 7.0.29,
PHP versions 7.1.x prior to 7.1.16 on Windows.

Vulnerability Insight
The flaw exists as the dumpable FPM child processes allow bypassing opcache access controls

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Security Bypass Vulnerability May18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813161
Version used: `$Revision: 12120 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.31`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2018-10545
Other:
  URL:http://www.php.net/ChangeLog-5.php#5.6.35
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
    URL:http://www.php.net/ChangeLog-7.php#7.0.29
    URL:http://www.php.net/ChangeLog-7.php#7.1.16
    URL:http://www.php.net/ChangeLog-7.php#7.2.4
```

Low (CVSS: 3.5)
NVT: phpMyAdmin Multiple Cross-Site Scripting Vulnerabilities - Nov14 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

phpMyAdmin is prone to multiple cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.10.1
```

Solution

Solution type: VendorFix

Update to version 4.2.10.1, 4.1.14.6 or 4.0.10.5.

Affected Software/OS

phpMyAdmin 4.2.x prior to 4.2.10.1, 4.1.x prior to 4.1.14.6, and 4.0.x prior to 4.0.10.5.

Vulnerability Insight

phpMyAdmin is prone ot multiple cross-site scripting (XSS) vulnerabilities that allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) database name or (2) table name, related to the libraries/DatabaseInterface.class.php code for SQL debug output and the js/server_status_monitor.js code for the server monitor page.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `phpMyAdmin Multiple Cross-Site Scripting Vulnerabilities - Nov14 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.112012

Version used: `$Revision: 12106 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2014-8326
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:70731
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2014-12/
```

Low (CVSS: 3.5)
NVT: phpMyAdmin Multiple Cross-Site Scripting Vulnerabilities - Oct14 (Windows)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

phpMyAdmin is prone to multiple cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.7.1
Fixed version:     4.2.9.1
```

Solution

Solution type: VendorFix

Update to version 4.2.9.1, 4.1.14.5 or 4.0.10.4.

Affected Software/OS

phpMyAdmin 4.2.x prior to 4.2.9.1, 4.1.x prior to 4.1.14.5, and 4.0.x prior to 4.0.10.4.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: phpMyAdmin Multiple Cross-Site Scripting Vulnerabilities - Oct14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.112014
Version used: $Revision: 12106 $

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2014-7217
BID:70252
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2014-11/
```

[return to 192.168.0.4]

Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
192.168.0.4|cpe:/a:apache:apr-util:1.5.3
192.168.0.4|cpe:/a:apache:http_server:2.4.10
192.168.0.4|cpe:/a:apache:portable_runtime:1.5.1
192.168.0.4|cpe:/a:apachefriends:xampp
192.168.0.4|cpe:/a:jquery:jquery:1.8.3
192.168.0.4|cpe:/a:oracle:mysql
192.168.0.4|cpe:/a:php:php:5.4.31
192.168.0.4|cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
192.168.0.4|cpe:/o:microsoft:windows_xp
```

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 14324 $`

References

```
Other:
  URL:http://cpe.mitre.org/
```

[return to 192.168.0.4]

Log 3306/tcp

Log (CVSS: 0.0)
NVT: MySQL/MariaDB Detection

Summary

Detects the installed version of MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner and store the information in KB.

Vulnerability Detection Result

```
Detected MySQL
Version:  unknown
Location: 3306/tcp
CPE:      cpe:/a:oracle:mysql
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Extra information:
Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MySQL server.
Some tests may fail. Allow the scanner to access the remote MySQL server for bet
↪ter results.
```

Log Method

Details: `MySQL/MariaDB Detection`
OID:1.3.6.1.4.1.25623.1.0.100152
Version used: `$Revision: 10929 $`

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A MySQL server is running on this port
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

Log 5800/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The Hostname/IP "192.168.0.4" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.0.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://192.168.0.4:5800/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method

Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 13679 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The Hostname/IP "192.168.0.4" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.0.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://192.168.0.4:5800/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 13679 $

References

Other:
  URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary

This plugin uses nikto to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 192.168.0.4:5800
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Log Method

Details: `Nikto (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: `$Revision: 13985 $`

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

... continues on next page ...

. . . continued from previous page . . .

Log Method

Details: `Services`

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary

This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
The wapiti report filename is empty. That could mean that a wrong version of wap
↪iti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapi
↪ti 1.x is not supported.
In short: Check the installation of wapiti and the scanner.
```

Log Method

Details: `wapiti (NASL wrapper)`

OID:1.3.6.1.4.1.25623.1.0.80110

Version used: `$Revision: 13985 $`

[return to 192.168.0.4]

Log 8080/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary

This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Log Method

Details: `Check open ports`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `$Revision: 13783 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
An unknown service is running on this port.
It is usually reserved for HTTP-Alt
```

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

Log 5900/tcp

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result

```
The remote VNC server chose security type #2 (VNC authentication)
```

Log Method
Details: `VNC security types`
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.

. . . continues on next page . . .

... continued from previous page ...

This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result

```
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.006
```

Solution

Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method

Details: `VNC Server and Protocol Version Detection`
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

Log 8181/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "192.168.0.4" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
not found
Requests to this service are done via HTTP/1.1.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
```

... continues on next page ...

. . . continued from previous page . . .

```
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://192.168.0.4:8181/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://192.168.0.4:8181/iconcache
```

Log Method

Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 13679 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method

Details: `HTTP Security Headers Detection`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

```
The remote web server type is :
Home Web Server (HWS164)
```

Solution

- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 11585 $`

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary

This plugin uses nikto to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
The target server did not return 404 on requests for non-existent pages.
This scan has not been executed since Nikto is prone to reporting many false pos
↪itives in this case.
```

... continues on next page ...

. . . continued from previous page . . .

```
If you wish to force this scan, you can enable it in the preferences of this scr
↪ipt.
```

Log Method

Details: `Nikto (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: `$Revision: 13985 $`

Log (CVSS: 0.0)
NVT: No 404 check

Summary

Remote web server does not reply with 404 error code.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Vulnerability Insight

This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead.
The Scanner enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate

Log Method

Details: `No 404 check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `$Revision: 13679 $`

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary

This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
The wapiti report filename is empty. That could mean that a wrong version of wap
↪iti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapi
↪ti 1.x is not supported.
In short: Check the installation of wapiti and the scanner.
```

Log Method

Details: `wapiti (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: `$Revision: 13985 $`

[return to 192.168.0.4]

Log 25/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
An SMTP server is running on this port
Here is its banner :
220 Mercury 4.51 ESMTP server ready.
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: SMTP Missing Support For STARTTLS

Summary
The remote SMTP server does not support the 'STARTTLS' command.

Vulnerability Detection Result

```
The remote SMTP server does not support the 'STARTTLS' command.
```

Log Method
Details: `SMTP Missing Support For STARTTLS`
OID:1.3.6.1.4.1.25623.1.0.105091
Version used: `$Revision: 13153 $`

Log (CVSS: 0.0)
NVT: SMTP Server type and version

Summary
This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.

Vulnerability Detection Result

```
Remote SMTP server banner:
220 Mercury 4.51 ESMTP server ready.
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) via an unencrypted connection:
HELP, SIZE 0, TIME
```

Log Method
Details: `SMTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: `$Revision: 14004 $`

[return to 192.168.0.4]

Log 443/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
An unknown service is running on this port.
It is usually reserved for HTTPS
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary

This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Nmap service detection (unknown) result for this port: https
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 443 192.168.0.4' and submit a possible collected fi
↪ngerprint to the nmap database.
```

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 192.168.0.4]

Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

Vulnerability Detection Result

```
A DCE endpoint resolution service seems to be running on this port.
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution

Solution type: Mitigation
Filter incoming traffic to this port.

Log Method

Details: `DCE/RPC and MSRPC Services Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: `$Revision: 11885 $`

[return to 192.168.0.4]

Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache APR Version Detection (Remote)

Summary

This script tries to detects the installed version of Apache APR from an exposed /server-info status page and sets the result in KB.

Vulnerability Detection Result

```
Detected Apache APR
Version:  1.5.1
Location: 80/tcp
CPE:      cpe:/a:apache:portable_runtime:1.5.1
Concluded from version/product identification result:
Server loaded APR Version:</strong> <tt>1.5.1</tt>
```

Log Method

Details: `Apache APR Version Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.111098
Version used: `$Revision: 6065 $`

Log (CVSS: 0.0)
NVT: Apache APR Version Detection (Remote)

Summary

This script tries to detects the installed version of Apache APR from an exposed /server-info status page and sets the result in KB.

Vulnerability Detection Result

```
Detected Apache APR-Utils
Version:  1.5.3
Location: 80/tcp
CPE:      cpe:/a:apache:apr-util:1.5.3
Concluded from version/product identification result:
Server loaded APU Version:</strong> <tt>1.5.3</tt>
```

Log Method

Details: `Apache APR Version Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.111098
Version used: `$Revision: 6065 $`

Log (CVSS: 0.0)
NVT: Apache Web Server Detection

Summary

Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result

```
Detected Apache
Version:  2.4.10
Location: 80/tcp
CPE:      cpe:/a:apache:http_server:2.4.10
Concluded from version/product identification result:
Server: Apache/2.4.10
```

Log Method

Details: `Apache Web Server Detection`
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: `$Revision: 10290 $`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:

. . . continues on next page . . .

. . . continued from previous page . . .

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "192.168.0.4" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
A possible recursion was detected during CGI scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
http://192.168.0.4/phpmyadmin/ (themes/dot.gif)
http://192.168.0.4/phpmyadmin/?D=A (themes/dot.gif)
http://192.168.0.4/phpmyadmin/doc/html/ (_sources/index.txt)
http://192.168.0.4/phpmyadmin/doc/html/ (_static/default.css)
http://192.168.0.4/phpmyadmin/doc/html/ (_static/doctools.js)
The following directories were used for CGI scanning:
http://192.168.0.4/
http://192.168.0.4/cgi-bin
http://192.168.0.4/error
http://192.168.0.4/login
http://192.168.0.4/phpmyadmin
http://192.168.0.4/phpmyadmin/doc/html
http://192.168.0.4/phpmyadmin/doc/html/_sources
http://192.168.0.4/phpmyadmin/doc/html/_static
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://192.168.0.4/phpmyadmin/doc/html/setup
http://192.168.0.4/phpmyadmin/setup
http://192.168.0.4/restricted
http://192.168.0.4/server-info
http://192.168.0.4/server-status
http://192.168.0.4/webalizer
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://192.168.0.4/icons
http://192.168.0.4/phpmyadmin/js
http://192.168.0.4/phpmyadmin/js/jquery
http://192.168.0.4/phpmyadmin/themes
http://192.168.0.4/phpmyadmin/themes/original
http://192.168.0.4/phpmyadmin/themes/original/img
http://192.168.0.4/phpmyadmin/themes/pmahomme
http://192.168.0.4/phpmyadmin/themes/pmahomme/img
http://192.168.0.4/phpmyadmin/themes/pmahomme/jquery
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.0.4/ (core.c [] providers [] mod_proxy_ajp.c [] http_core.c [] mo
↪d_include.c [] mod_isapi.c [] mod_win32.c [] mod_rewrite.c [] mod_cgi.c [] mod
↪_authz_core.c [] mod_auth_basic.c [] mod_cache_disk.c [] mod_dir.c [] config [
↪] mod_access_compat.c [] mod_dav_lock.c [] mod_authz_host.c [] mod_authz_group
↪file.c [] mod_mime.c [] mpm_winnt.c [] mod_so.c [] mod_allowmethods.c [] mod_p
↪roxy.c [] mod_log_config.c [] mod_actions.c [] mod_authn_core.c [] mod_headers
↪.c [] mod_negotiation.c [] mod_asis.c [] mod_php5.c [] mod_status.c [] server
↪[] mod_info.c [] mod_autoindex.c [] mod_authn_file.c [] mod_env.c [] mod_seten
↪vif.c [] mod_socache_shmcb.c [] mod_alias.c [] hooks [] list [] mod_authz_user
↪.c [] )
http://192.168.0.4/phpmyadmin/db_create.php (lang [en] collation_connection [utf
↪8mb4_unicode_ci] token [1a275c78532d670f938daf983afbb39a] reload [1] new_db []
↪ db_collation [] )
http://192.168.0.4/phpmyadmin/db_operations.php (token [e1429de086a59eae37ddfcf3
↪b513213b] db [cdcol] server [1] )
http://192.168.0.4/phpmyadmin/db_structure.php (token [e1429de086a59eae37ddfcf3b
↪513213b] collation_connection [utf8mb4_unicode_ci] favorite_table [1] ajax_req
↪uest [1] lang [en] db [cdcol] server [1] sync_favorite_tables [1] )
http://192.168.0.4/phpmyadmin/doc/html/search.html (check_keywords [yes] q [] ar
↪ea [default] )
http://192.168.0.4/phpmyadmin/export.php (lang [en] collation_connection [utf8mb
↪4_unicode_ci] token [80f494e653efc96c57844e1946a60c4f] export_type [server] ex
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪port_method [quick] quick_or_custom [quick] quick_or_custom [custom] db_select
↪[] [] output_format [sendit] filename_template [@SERVER@] remember_template []
↪ charset_of_file [] compression [] output_format [astext] maxsize [] what [] c
↪odegen_structure_or_data [data] codegen_format [] csv_separator [,] csv_enclos
↪ed [&quot;] csv_escaped [&quot;] csv_terminated [AUTO] csv_null [NULL] csv_rem
↪oveCRLF [something] csv_columns [something] csv_structure_or_data [data] excel
↪_null [NULL] excel_removeCRLF [something] excel_columns [something] excel_edit
↪ion [] excel_structure_or_data [data] htmlword_structure_or_data [structure] h
↪tmlword_structure_or_data [data] htmlword_structure_or_data [structure_and_dat
↪a] htmlword_null [NULL] htmlword_columns [something] json_structure_or_data [d
↪ata] latex_caption [something] latex_structure_or_data [structure] latex_struc
↪ture_or_data [data] latex_structure_or_data [structure_and_data] latex_structu
↪re_caption [Structure of table @TABLE@] latex_structure_continued_caption [Str
↪ucture of table @TABLE@ (continued)] latex_structure_label [tab:@TABLE@-struct
↪ure] latex_relation [something] latex_comments [something] latex_mime [somethi
↪ng] latex_columns [something] latex_data_caption [Content of table @TABLE@] la
↪tex_data_continued_caption [Content of table @TABLE@ (continued)] latex_data_l
↪abel [tab:@TABLE@-data] latex_null [\textit{NULL}] mediawiki_structure_or_data
↪ [structure] mediawiki_structure_or_data [data] mediawiki_structure_or_data [s
↪tructure_and_data] mediawiki_caption [something] mediawiki_headers [something]
↪ ods_null [NULL] ods_columns [something] ods_structure_or_data [data] odt_stru
↪cture_or_data [structure] odt_structure_or_data [data] odt_structure_or_data [
↪structure_and_data] odt_relation [something] odt_comments [something] odt_mime
↪ [something] odt_columns [something] odt_null [NULL] pdf_report_title [] pdf_s
↪tructure_or_data [data] phparray_structure_or_data [data] sql_include_comments
↪ [something] sql_header_comment [] sql_dates [something] sql_relation [somethi
↪ng] sql_mime [something] sql_use_transaction [something] sql_disable_fk [somet
↪hing] sql_views_as_tables [something] sql_compatibility [] sql_drop_database [
↪something] sql_structure_or_data [structure] sql_structure_or_data [data] sql_
↪structure_or_data [structure_and_data] sql_create_database [something] sql_dro
↪p_table [something] sql_create_table [something] sql_create_view [something] s
↪ql_procedure_function [something] sql_create_trigger [something] sql_create_ta
↪ble_statements [something] sql_if_not_exists [something] sql_auto_increment [s
↪omething] sql_backquotes [something] sql_truncate [something] sql_delayed [som
↪ething] sql_ignore [something] sql_type [] sql_insert_syntax [complete] sql_in
↪sert_syntax [extended] sql_insert_syntax [both] sql_insert_syntax [none] sql_m
↪ax_query_size [50000] sql_hex_for_binary [something] sql_utc_time [something]
↪texytext_structure_or_data [structure] texytext_structure_or_data [data] texyt
↪ext_structure_or_data [structure_and_data] texytext_columns [something] texyte
↪xt_null [NULL] yaml_structure_or_data [data] )
http://192.168.0.4/phpmyadmin/import.php (sql_no_auto_value_on_zero [something]
↪bkm_label [] token [214a1098ecdf86d77de7bd333502acaa] message_to_show [Your SQ
↪L query has been executed successfully.] SQL [Go] allow_interrupt [yes] goto [
↪server_sql.php] csv_enclosed [&quot;] LockFromUpdate [] MAX_FILE_SIZE [2097152
↪] ods_recognize_currency [something] noplugin [6377d9db4c91c] focus_querywindo
↪w [true] retain_query_box [1] csv_terminated [,] import_type [server] collatio
↪n_connection [utf8mb4_unicode_ci] show_query [1] sql_compatibility [] ods_empt
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪y_rows [something] csv_new_line [auto] pos [0] bkm_replace [true] ods_recogniz
↪e_percentages [something] csv_col_names [something] csv_replace [something] fo
↪rmat [] lang [en] prev_sql_query [] sql_delimiter [;] csv_ignore [something] s
↪kip_queries [0] charset_of_file [] is_js_confirmed [0] import_file [] csv_esca
↪ped [&quot;] bkm_all_users [true] ods_col_names [something] )
http://192.168.0.4/phpmyadmin/index.php (phpMyAdmin [47dmo5fk081l7310nkc81jqt4s8
↪j3sct] token [e1429de086a59eae37ddfcf3b513213b] target [] table [] set_theme [
↪] reload [1] collation_connection [utf8mb4_unicode_ci] set_fontsize [] lang [e
↪n] db [] server [1] )
http://192.168.0.4/phpmyadmin/js/get_image.js.php (theme [pmahomme] )
http://192.168.0.4/phpmyadmin/js/get_scripts.js.php (token [e1429de086a59eae37dd
↪fcf3b513213b] collation_connection [utf8mb4_unicode_ci] lang [en] scripts[] [c
↪odemirror/addon/runmode/runmode.js] )
http://192.168.0.4/phpmyadmin/js/messages.php (token [e1429de086a59eae37ddfcf3b5
↪13213b] collation_connection [utf8mb4_general_ci] lang [en] db [] )
http://192.168.0.4/phpmyadmin/navigation.php (token [e1429de086a59eae37ddfcf3b51
↪3213b] collation_connection [utf8mb4_unicode_ci] ajax_request [1] lang [en] )
http://192.168.0.4/phpmyadmin/phpmyadmin.css.php (token [e1429de086a59eae37ddfcf
↪3b513213b] collation_connection [utf8mb4_unicode_ci] lang [en] nocache [586192
↪3964ltr] server [1] )
http://192.168.0.4/phpmyadmin/prefs_forms.php (Servers-1-hide_db [] token [ae464
↪7f1d9fa52700aedf37bb9730c7f] tab_hash [] CharTextareaRows [2] TitleTable [@HTT
↪P_HOST@ / @VSERVER@ / @DATABASE@ / @TABLE@ | @PHPMYADMIN@] VersionCheck [] Sen
↪dErrorReports [] CharTextareaCols [40] TitleDatabase [@HTTP_HOST@ / @VSERVER@
↪/ @DATABASE@ | @PHPMYADMIN@] target [] DisableMultiTableMaintenance [] submit_
↪reset [Reset] CharEditing [] TitleDefault [@HTTP_HOST@ | @PHPMYADMIN@] table [
↪] MaxSizeForInputField [60] TitleServer [@HTTP_HOST@ / @VSERVER@ | @PHPMYADMIN
↪@] PmaNoRelation_DisableWarning [] collation_connection [utf8mb4_unicode_ci] L
↪oginCookieValidity [1440] submit_save [Apply] ServerLibraryDifference_DisableW
↪arning [] lang [en] MaxTableList [250] NumFavoriteTables [10] MinSizeForInputF
↪ield [4] InitialSlidersState [] MaxDbList [100] server [1] db [] NumRecentTabl
↪es [10] ShowHint [] LongtextDoubleTextarea [] ReservedWordDisableWarning [] Na
↪turalOrder [] TextareaRows [15] SuhosinDisableWarning [] form [Features] check
↪_page_refresh [] SkipLockedTables [] TextareaCols [40] )
http://192.168.0.4/phpmyadmin/prefs_manage.php (submit_export [Go] token [e1429d
↪e086a59eae37ddfcf3b513213b] json [] import_merge [] target [] submit_clear [Re
↪set] table [] MAX_FILE_SIZE [2097152] collation_connection [utf8mb4_unicode_ci
↪] import_type [local_storage] export_type [local_storage] lang [en] server [1]
↪ db [] import_file [] submit_import [Go] )
http://192.168.0.4/phpmyadmin/querywindow.php (token [e1429de086a59eae37ddfcf3b5
↪13213b] table [] sql_query [] collation_connection [utf8mb4_unicode_ci] queryd
↪isplay_tab [sql] lang [en] db [] no_js [true] )
http://192.168.0.4/phpmyadmin/server_collations.php (token [e1429de086a59eae37dd
↪fcf3b513213b] target [] table [] collation_connection [utf8mb4_unicode_ci] lan
↪g [en] server [1] db [] )
http://192.168.0.4/phpmyadmin/server_databases.php (token [e1429de086a59eae37ddf
↪cf3b513213b] selected_dbs[] [webauth] target [] table [] sort_order [desc] col
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪lation_connection [utf8mb4_unicode_ci] pos [0] sort_by [SCHEMA_NAME] lang [en]
↪ db [] server [1] dbstats [0] )
http://192.168.0.4/phpmyadmin/server_engines.php (token [e1429de086a59eae37ddfcf
↪3b513213b] engine [FEDERATED] target [] table [] collation_connection [utf8mb4
↪_unicode_ci] lang [en] page [Status] db [] server [1] )
http://192.168.0.4/phpmyadmin/server_export.php (token [e1429de086a59eae37ddfcf3
↪b513213b] target [] table [] collation_connection [utf8mb4_unicode_ci] lang [e
↪n] db [] server [1] )
http://192.168.0.4/phpmyadmin/server_import.php (token [e1429de086a59eae37ddfcf3
↪b513213b] target [] table [] collation_connection [utf8mb4_unicode_ci] lang [e
↪n] server [1] db [] )
http://192.168.0.4/phpmyadmin/server_privileges.php (token [e1429de086a59eae37dd
↪fcf3b513213b] tablename [] checkprivsdb [cdcol] target [] table [] hostname [%
↪25] selected_usr[] [root&amp;amp;#27;localhost] username [] delete [Go] flush_
↪privileges [1] dbname [] collation_connection [utf8mb4_unicode_ci] mode [2] in
↪itial [] lang [en] drop_users_db [] server [1] db [] adduser [1] viewing_mode
↪[server] export [1] )
http://192.168.0.4/phpmyadmin/server_replication.php (token [e1429de086a59eae37d
↪dfcf3b513213b] target [] table [] mr_configure [1] sl_configure [1] collation_
↪connection [utf8mb4_unicode_ci] lang [en] server [1] db [] repl_clear_scr [1]
↪)
http://192.168.0.4/phpmyadmin/server_sql.php (token [e1429de086a59eae37ddfcf3b51
↪3213b] target [] table [] collation_connection [utf8mb4_unicode_ci] lang [en]
↪server [1] db [] )
http://192.168.0.4/phpmyadmin/server_status.php (token [e1429de086a59eae37ddfcf3
↪b513213b] kill [44] column_name [ID] target [] table [] sort_order [ASC] colla
↪tion_connection [utf8mb4_unicode_ci] full [1] lang [en] order_by_field [Id] db
↪ [] server [1] )
http://192.168.0.4/phpmyadmin/server_status_advisor.php (token [95527ef3441bccae
↪c0e4b8ecc3dbe483] target [] table [] collation_connection [utf8mb4_unicode_ci]
↪ lang [en] server [1] db [] )
http://192.168.0.4/phpmyadmin/server_status_monitor.php (token [95527ef3441bccae
↪c0e4b8ecc3dbe483] target [] table [] collation_connection [utf8mb4_unicode_ci]
↪ lang [en] db [] server [1] )
http://192.168.0.4/phpmyadmin/server_status_queries.php (token [95527ef3441bccae
↪c0e4b8ecc3dbe483] target [] table [] collation_connection [utf8mb4_unicode_ci]
↪ lang [en] db [] server [1] )
http://192.168.0.4/phpmyadmin/server_status_variables.php (token [95527ef3441bcc
↪aec0e4b8ecc3dbe483] flush [TABLES] collation_connection [utf8mb4_unicode_ci] f
↪ilterCategory [] dontFormat [] lang [en] filterAlert [] filterText [] )
http://192.168.0.4/phpmyadmin/server_variables.php (token [e1429de086a59eae37ddf
↪cf3b513213b] target [] table [] collation_connection [utf8mb4_unicode_ci] lang
↪ [en] db [] server [1] )
http://192.168.0.4/phpmyadmin/setup/ (D [A] token [125e2dc51cdea6c0e43416ef1a699
↪f4a] version_check [1] formset [Features] collation_connection [utf8_general_c
↪i] lang [] page [form] )
http://192.168.0.4/phpmyadmin/setup/config.php (token [125e2dc51cdea6c0e43416ef1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪a699f4a] tab_hash [] submit_clear [Clear] ServerDefault [] submit_download [Do
↪wnload] submit_delete [Delete] submit_load [Load] collation_connection [utf8_g
↪eneral_ci] submit_save [Save] lang [en] submit_display [Display] eol [] Defaul
↪tLang [] )
http://192.168.0.4/phpmyadmin/setup/index.php (token [125e2dc51cdea6c0e43416ef1a
↪699f4a] tab_hash [] submit [New server] collation_connection [utf8_general_ci]
↪ lang [] mode [add] page [servers] check_page_refresh [] )
http://192.168.0.4/phpmyadmin/sql.php (token [e1429de086a59eae37ddfcf3b513213b]
↪goto [server_status_variables.php] target [] table [users] sql_query [SHOW+OPE
↪N+TABLES] collation_connection [utf8mb4_unicode_ci] lang [en] db [login] serve
↪r [1] )
http://192.168.0.4/phpmyadmin/url.php (url [http%3A%2F%2Fdev.mysql.com%2Fdoc%2Fr
↪efman%2F5.5%2Fen%2Findex.html] )
```

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 13679 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result

```
The following apps/services were identified:
"phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://192.168.0.4/p
↪hpmyadmin/favicon.ico"
```

Impact
The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details: `Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `$Revision: 11730 $`

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result

```
The remote web server type is :
Apache/2.4.10 (Win32) PHP/5.4.31
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
```

Solution
- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 11585 $`

Log (CVSS: 0.0)
NVT: HTTP TRACE

Summary

Transparent or reverse HTTP proxies may be implement on some sites.

Vulnerability Detection Result

```
The TRACE method revealed 1 proxy(s) between us and the web server :
? - Apache/2.4.10 (Win32) PHP/5.4.31
```

Log Method

Details: `HTTP TRACE`
OID:1.3.6.1.4.1.25623.1.0.11040
Version used: `$Revision: 13660 $`

Log (CVSS: 0.0)
NVT: jQuery Detection

Summary

Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.

Vulnerability Detection Result

```
Detected jQuery
Version:  1.8.3
Location: /phpmyadmin/js/get_scripts.js.php?lang=en&amp;collation_connection=utf
↪8mb4_unicode_ci&amp;token=87fa8496d881c7727e7a8d9f0511f49f&amp;scripts[]=jquer
↪y
CPE:      cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="js/get_scripts.js.php?lang=en&amp;collation_connection=utf8mb4_unicode_ci&a
↪mp;token=87fa8496d881c7727e7a8d9f0511f49f&amp;scripts[]=jquery/jquery-1.8.3.mi
↪n.js
```

Log Method

Details: `jQuery Detection`
OID:1.3.6.1.4.1.25623.1.0.141622
Version used: `$Revision: 14001 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
Other:
  URL:https://jquery.com/
```

Log (CVSS: 0.0)
NVT: jQuery Detection

Summary

Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.

Vulnerability Detection Result

```
Detected jQuery
Version:  1.8.3
Location: /phpmyadmin/setup/../js/jquery
CPE:      cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="../js/jquery/jquery-1.8.3.min.js
```

Log Method

Details: `jQuery Detection`
OID:1.3.6.1.4.1.25623.1.0.141622
Version used: `$Revision: 14001 $`

References

```
Other:
  URL:https://jquery.com/
```

Log (CVSS: 0.0)
NVT: PHP Version Detection (Remote)

Summary

Detects the installed version of PHP. This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result

```
Detected PHP
Version:  5.4.31
Location: 80/tcp
CPE:      cpe:/a:php:php:5.4.31
Concluded from version/product identification result:
Server: Apache/2.4.10 (Win32) PHP/5.4.31
```

Log Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: PHP Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: $Revision: 13811 $

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

Summary
Detection of phpMyAdmin.
The script sends a connection request to the server and attempts to extract the version number from the reply.

Vulnerability Detection Result

```
Detected phpMyAdmin
Version:  4.2.7.1
Location: /phpmyadmin
CPE:      cpe:/a:phpmyadmin:phpmyadmin:4.2.7.1
Concluded from version/product identification result:
phpMyAdmin 4.2.7.1
Concluded from version/product identification location:
http://192.168.0.4/phpmyadmin/index.php
Extra information:
- Possible unprotected setup dir identified at http://192.168.0.4/phpmyadmin/set
↪up/
```

Log Method
Details: phpMyAdmin Detection
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: $Revision: 12754 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary

This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
The wapiti report filename is empty. That could mean that a wrong version of wap
↪iti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapi
↪ti 1.x is not supported.
In short: Check the installation of wapiti and the scanner.
```

Log Method

Details: `wapiti (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: `$Revision: 13985 $`

Log (CVSS: 0.0)
NVT: XAMPP Version Detection

Summary

This script finds the installed XAMPP version and saves the version in KB.

Vulnerability Detection Result

```
Detected XAMPP
Version:  unknown
Location: /dashboard
CPE:      cpe:/a:apachefriends:xampp
Concluded from version/product identification location:
http://192.168.0.4/xampp/start.php
```

Log Method

Details: `XAMPP Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900526
Version used: `$Revision: 8141 $`

[return to 192.168.0.4]

Log 21/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `$Revision: 13783 $`

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects and reports a FTP Server Banner.

Vulnerability Detection Result

```
Remote FTP server banner:
220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@163.com)
220- Welcome to Easy FTP Server
220
This is probably:
- Easy~FTP Server
Server operating system information collected via "SYST" command:
215 UNIX Type: L8
Server status information collected via "STAT" command:
211- Status for user anonymous from 192.168.0.50
211 End of status.
```

Log Method
Details: `FTP Banner Detection`
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: `$Revision: 13637 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
An unknown service is running on this port.
It is usually reserved for FTP
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result

```
A SMB server is running on this port
```

Log Method

Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary

This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Best matching OS:
OS: Windows XP
CPE: cpe:/o:microsoft:windows_xp
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows 5.1; SMB Str
↪ing: Windows 2000 LAN Manager
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.10 (Win32)
↪PHP/5.4.31
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
```

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 14244 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: SMB Registry : Windows Build Number and Service Pack Version

Summary

Detection of the installed Windows build number and Service Pack version.
The script logs in via SMB, reads various registry keys to retrieve the Windows build number and Service Pack version.

Vulnerability Detection Result

```
It was not possible to access the registry key 'SYSTEM\CurrentControlSet\Control
↪\Session Manager\Environment' due to e.g. missing access permissions of the sc
↪anning user. Authenticated scans might be incomplete, please check the referen
↪ces how to correctly configure the user account for Authenticated scans.
```

Log Method

Details: `SMB Registry : Windows Build Number and Service Pack Version`
OID:1.3.6.1.4.1.25623.1.0.10401

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 12772 $`

References

```
Other:
  URL:https://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.htm
↪l#requirements-on-target-systems-with-windows
```

Log (CVSS: 0.0)
NVT: Traceroute

Summary

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 172.17.0.2 to 192.168.0.4:
172.17.0.2
192.168.0.4
```

Solution

Block unwanted packets from escaping your network.

Log Method

Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary

This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://community.greenbone.net/c/vulnera
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪bility-tests:
Banner: Server: Home Web Server (HWS164)
Identified from: HTTP Server banner on port 8181/tcp
Banner: 220 Mercury 4.51 ESMTP server ready.
Identified from: SMTP banner on port 25/tcp
```

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 192.168.0.4]

Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary

Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result

```
SMB signing is disabled on this host
```

Log Method

Details: `Microsoft SMB Signing Disabled`
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: `$Revision: 11003 $`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary

The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result

```
The following shares were found
IPC$
```

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method

Details: `Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `$Revision: 11420 $`

Log (CVSS: 0.0)
NVT: SMB log in

Summary

This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result

```
It was possible to log into the remote host using the SMB protocol.
```

Log Method

Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `$Revision: 13247 $`

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

Summary

It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Log Method

Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `$Revision: 13248 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary

It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result

```
Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 2000 LAN Manager
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected OS: Windows 5.1
```

Log Method

Details: `SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 13813 $`

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary

Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result

```
Only SMBv1 is enabled on remote target
```

Log Method

Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `$Revision: 10898 $`

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary

This script reports information about the SMB server of the remote host collected with the 'smbclient' tool.

Vulnerability Detection Result

```
OS Version = WINDOWS 5.1
Domain = OS=[WINDOWS 5.1
SMB Serverversion = WINDOWS 2000 LAN MANAGER
```

Log Method

Details: `SMB Test with 'smbclient'`
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: `$Revision: 13274 $`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result

```
A CIFS server is running on this port
```

Log Method

Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 13541 $`

[return to 192.168.0.4]

This file was automatically generated.