Scan Report

August 7, 2019

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 "linuxvm scan". The scan started at Tue Aug 6 04:53:02 2019 UTC and ended at Tue Aug 6 07:03:40 2019 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

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.57.5	64	89	8	0	0
Total: 1	64	89	8	0	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.
It only lists hosts that produced issues.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 161 results selected by the filtering described above. Before filtering there were 232 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.57.5

Host scan start Tue Aug 6 04:53:40 2019 UTC
Host scan end Tue Aug 6 07:03:39 2019 UTC

Service (Port)	Threat Level
445/tcp	High
3500/tcp	High
21/tcp	High
80/tcp	High
22/tcp	High
general/tcp	Medium
631/tcp	Medium
445/tcp	Medium
3500/tcp	Medium
21/tcp	Medium
80/tcp	Medium

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Low
445/tcp	Low
21/tcp	Low
80/tcp	Low
22/tcp	Low

2.1.1 High 445/tcp

High (CVSS: 7.5)
NVT: Samba Server 'CVE-2017-14746' Use-after-free Vulnerability

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to a use-after-free vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.5.15
Installation
path / port:       445/tcp
```

Impact

A malicious SMB1 request can be used to control the contents of heap memory via a deallocated heap pointer. It is possible this may be used to compromise the SMB server.

Solution

Solution type: VendorFix

Update to Samba 4.5.15, 4.6.11, 4.7.3 or later. Workaround:
Prevent SMB1 access to the server by setting the parameter:
server min protocol = SMB2
to the [global] section of your smb.conf and restart smbd. This prevents a SMB1 access to the server. Note this could cause older clients to be unable to connect to the server.

Affected Software/OS

Samba versions 4.0.0 to 4.5.14, 4.6.x prior to 4.6.11, 4.7.x prior to 4.7.3 with enabled SMBv1 support.

Vulnerability Insight

The flaw exists due to a client which may use an SMB1 request to manipulate the contents of heap space.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba Server 'CVE-2017-14746' Use-after-free Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108294
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-14746
BID:101907
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-14746.html
```

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

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

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

Vulnerability Detection Result

```
The "Samba" version on the remote host has reached the end of life.
CPE:               cpe:/a:samba:samba:4.3.11
Installed version: 4.3.11
Location/URL:      445/tcp
EOL version:       4.3
EOL date:          2017-03-07
```

Impact

An end of life version of Samba 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 Samba version on the remote host to a still supported version.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.140159
Version used: `$Revision: 11923 $`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
Other:
  URL:https://wiki.samba.org/index.php/Samba_Release_Planning
```

High (CVSS: 10.0)
NVT: Samba Remote Code Execution Vulnerability (SambaCry)

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary
This host is running Samba and is prone to remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.4.14 or apply patch
Installation
path / port:       445/tcp
```

Impact
Successfully exploiting this issue will allow remote attackers to execute arbitrary code as root on an affected system.

Solution
Solution type: VendorFix
Upgrade to Samba 4.6.4 or 4.5.10 or 4.4.14 or later.

Affected Software/OS
All Samba Server versions 3.5.0 onwards,
Samba Server versions 4.4.x before 4.4.14,
Samba Server versions 4.5.x before 4.5.10, and

. . . continues on next page . . .

. . . continued from previous page . . .

Samba Server versions 4.6.x before 4.6.4

Vulnerability Insight

The flaw exists due to an input validation error, which allows a malicious client to upload a shared library to a writable share.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba Remote Code Execution Vulnerability (SambaCry)`
OID:1.3.6.1.4.1.25623.1.0.811055
Version used: `$Revision: 11888 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-7494
BID:98636
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-7494.html
   URL:http://hackaday.com/2017/05/25/linux-sambacry/
   URL:http://thehackernews.com/2017/05/samba-rce-exploit.html
   URL:https://github.com/omri9741/cve-2017-7494
```

[return to 192.168.57.5]

2.1.2 High 3500/tcp

High (CVSS: 7.5)
NVT: Ruby on Rails Action Pack Remote Code Execution Vulnerability (Linux)

Product detection result

```
cpe:/a:ruby-lang:ruby:2.3.7
Detected by Ruby on Rails Version Detection (OID: 1.3.6.1.4.1.25623.1.0.902089)
```

Summary

This host is running Ruby on Rails and is prone to remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.4
Fixed version:     4.2.5.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow a remote attacker to control the arguments of the render method in a controller or a view, resulting in the possibility of executing arbitrary ruby code.

Solution

Solution type: VendorFix

Upgrade to Ruby on Rails 3.2.22.2 or 4.1.14.2 or 4.2.5.2 or later.

Affected Software/OS

Ruby on Rails before 3.2.22.2, Ruby on Rails 4.x before 4.1.14.2 and Ruby on Rails 4.2.x before 4.2.5.2 on Linux.

Vulnerability Insight

The flaw is due to an improper sanitization of user supplied inputs to the 'render' method in a controller or view by 'Action Pack'.

Vulnerability Detection Method

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

Details: `Ruby on Rails Action Pack Remote Code Execution Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809353

Version used: `2019-07-05T10:16:38+0000`

Product Detection Result

Product: `cpe:/a:ruby-lang:ruby:2.3.7`

Method: `Ruby on Rails Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.902089)

References

```
CVE: CVE-2016-2098
BID:83725
Other:
  URL:https://www.debian.org/security/2016/dsa-3509
   URL:https://groups.google.com/forum/message/raw?msg=rubyonrails-security/ly-I
↪H-fxr_Q/WLoOhcMZIAAJ
```

[return to 192.168.57.5]

2.1.3 High 21/tcp

High (CVSS: 7.5)

NVT: ProFTPD <= 1.3.6 'mod_copy' Vulnerability

Product detection result

`cpe:/a:proftpd:proftpd:1.3.5`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)
```

Summary

An arbitrary file copy vulnerability in mod_copy in ProFTPD allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.

Vulnerability Detection Result

```
Installed version: 1.3.5
Fixed version:     None
```

Solution

Solution type: Workaround

As a workaround disable mod_copy in the ProFTPd configuration file.

Affected Software/OS

ProFTPD version 1.3.6 and prior.

Vulnerability Detection Method

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

Details: `ProFTPD <= 1.3.6 'mod_copy' Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.142662

Version used: `2019-07-24T05:45:03+0000`

Product Detection Result

Product: `cpe:/a:proftpd:proftpd:1.3.5`

Method: `ProFTPD Server Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.900815)

References

```
CVE: CVE-2019-12815
Other:
  URL:https://tbspace.de/cve201912815proftpd.html
   URL:http://bugs.proftpd.org/show_bug.cgi?id=4372
   URL:https://www.bleepingcomputer.com/news/security/proftpd-vulnerability-lets
↪-users-copy-files-without-permission/
```

[return to 192.168.57.5]

2.1.4 High 80/tcp

High (CVSS: 7.1)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.5.28
```

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808613
Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 7.2)
NVT: PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.28/5.5.12
```

Impact

Successful exploitation will allow remote attackers to gain access to the socket and gain elevated privileges.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.28 or 5.5.12 or later.

Affected Software/OS

PHP versions 5.4.x before 5.4.28 and 5.5.x before 5.5.12.

Vulnerability Insight

The flaw is due to error in 'sapi/fpm/fpm/fpm_unix.c' within FastCGI Process Manager that sets insecure permissions for a unix socket.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.804290
Version used: `$Revision: 12391 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-0185
BID:67118
Other:
  URL:http://seclists.org/oss-sec/2014/q2/192
    URL:http://www.php.net/archive/2014.php#id2014-05-01-1
```

. . . continues on next page . . .

. . . continued from previous page . . .

URL:http://www.openwall.com/lists/oss-security/2014/04/29/5
URL:http://php.net

High (CVSS: 7.5)
NVT: PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.3.28/5.4.23/5.5.7
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).

Solution

Solution type: VendorFix
Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.

Affected Software/OS

PHP versions before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7.

Vulnerability Insight

The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13`
OID:1.3.6.1.4.1.25623.1.0.804174
Version used: `$Revision: 11865 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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-2013-6420
Other:
  URL:http://secunia.com/advisories/56055
   URL:http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory
↪-Corruption.html
   URL:http://www.php.net
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

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 Vulnerabilities - 01 - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808788
Version used: `$Revision: 12431 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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 - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

. . . continues on next page . . .

. . . continued from previous page . . .

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 Linux

Vulnerability Insight
Multiple flaws are due to,
- Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script.
- A 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808199
Version used: `$Revision: 12051 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

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 'var_unserializer' Denial of Service Vulnerability (Linux)

Product detection result
```
cpe:/a:php:php:5.4.5
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: 5.4.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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.

Affected Software/OS

PHP versions prior to 5.6.26 on Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809321

Version used: `$Revision: 11938 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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 Multiple Vulnerabilities - Feb19 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.4.5
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)
- 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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142048

Version used: `$Revision: 13857 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 Multiple Vulnerabilities - 01 - Jul14

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.30/5.5.14
```

Impact

Successful exploitation will allow remote attackers to conduct denial of service attacks or potentially execute arbitrary code.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.30 or 5.5.14 or later.

Affected Software/OS

PHP version 5.4.x before 5.4.30 and 5.5.x before 5.5.14

Vulnerability Insight

The flaws exist due to,

- A buffer overflow in the 'mconvert' function in softmagic.c script.
- Two type confusion errors when deserializing ArrayObject and SPLObjectStorage objects.
- An unspecified boundary check issue in the 'cdf_read_short_sector' function related to Fileinfo.
- Some boundary checking issues in the 'cdf_read_property_info', 'cdf_count_chain' and 'cdf_check_stream_offset' functions in cdf.c related to Fileinfo.

Vulnerability Detection Method

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

Details: `PHP Multiple Vulnerabilities - 01 - Jul14`

OID:1.3.6.1.4.1.25623.1.0.804683

Version used: `$Revision: 11867 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-3478, CVE-2014-3515, CVE-2014-0207, CVE-2014-3487, CVE-2014-3479,
↪CVE-2014-3480
BID:68239, 68237, 68243, 68120, 68241, 68238
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://secunia.com/advisories/59575
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

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 Linux

Vulnerability Insight

Multiple flaws are due to,

- The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808790
Version used: `$Revision: 14181 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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 (Li.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.807505

Version used: `$Revision: 12431 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 7.5)

NVT: PHP 'libgd' Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809338
Version used: `$Revision: 11811 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
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
   URL:http://www.php.net
```

High (CVSS: 7.5)
NVT: Drupal Multiple Vulnerabilities-02 August15 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary
This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.39
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data, and execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

Solution

Solution type: VendorFix

Upgrade to version 7.39 or later.

Affected Software/OS

Drupal 7.x before 7.39 on Linux.

Vulnerability Insight

Multiple flaws exixts as,

- An error in the Ajax handler involving a whitelisted HTML element, possibly related to the 'a' tag.
- An error in the SQL comment filtering system in the Database API.

Vulnerability Detection Method

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

Details: `Drupal Multiple Vulnerabilities-02 August15 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.805967

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2015-6665, CVE-2015-6659
Other:
  URL:https://www.drupal.org/SA-CORE-2015-003
```

High (CVSS: 7.5)

NVT: PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15

Product detection result

```
cpe:/a:php:php:5.4.5
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 use-after-free vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 5.4.5
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:5.4.5`

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: 7.5)

NVT: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808634
Version used: `$Revision: 11938 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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-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: 7.5)
NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.6.34
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 Linux.

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `PHP Stack Buffer Overflow Vulnerability Mar18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812821
Version used: `$Revision: 12391 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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 Multiple Vulnerabilities - 02 - Jun15 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed Version:     5.4.41
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805660
Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: Apache HTTP Server Multiple Vulnerabilities June17 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
Fixed version:     2.4.26
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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 Linux.

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.811214

Version used: `2019-07-05T10:41:31+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

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
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
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807503
Version used: `$Revision: 12149 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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 Directory Traversal Vulnerability - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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

```
Installed version: 5.4.5
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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808617
Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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-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: 7.5)
NVT: Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-004) (Linux, Version Check)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

Drupal is prone to a remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.59
Installation
path / port:       /drupal
```

Solution

Solution type: VendorFix

Update to version 7.59, 8.4.8, 8.5.3 or later.

Affected Software/OS

Drupal 7.x and 8.x

Vulnerability Insight

A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised. This vulnerability is related to SA-CORE-2018-002 (CVE-2018-7600).

Vulnerability Detection Method

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

Details: `Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-004) (Li.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.141028

Version used: `$Revision: 12012 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2018-7602
Other:
  URL:https://www.drupal.org/sa-core-2018-004
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808794

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 11961 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: Drupal Core Multiple Vulnerabilities (SA-CORE-2017-003) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary
This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.56
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code, get or register a user account on the site with permissions to upload files into a private file system and modify the file resource.

Solution
Solution type: VendorFix
Upgrade to Drupal core version 7.56 or 8.3.4 or later.

Affected Software/OS
Drupal core version 7.x versions prior to 7.56 and 8.x versions prior to 8.3.4.

Vulnerability Insight
Multiple flaws are due to,
- PECL YAML parser does not handle PHP objects safely during certain operations within Drupal core.
- The file REST resource does not properly validate some fields when manipulating files.

. . . continues on next page . . .

. . . continued from previous page . . .

- Private files that have been uploaded by an anonymous user but not permanently attached to content on the site is visible to the anonymous user, Drupal core did not provide sufficient protection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Drupal Core Multiple Vulnerabilities (SA-CORE-2017-003) (Linux)`
OID:1.3.6.1.4.1.25623.1.0.810959
Version used: `$Revision: 13750 $`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2017-6920, CVE-2017-6921, CVE-2017-6922
BID:99211, 99222, 99219
Other:
  URL:https://www.drupal.org/SA-CORE-2017-003
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
PHP versions prior to 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Linux

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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808675
Version used: `$Revision: 12313 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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
BID:75291, 75292, 75244
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

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

Product detection result
```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.44
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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 Linux

Vulnerability Insight
The multiple flaws are due to,
- An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script.
- 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808604
Version used: `$Revision: 12313 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 7.5)
NVT: phpMyAdmin < 4.8.6 SQL Injection Vulnerability - PMASA-2019-3 (Linux)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.5.8
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to an SQL injection vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 3.5.8
Fixed version:     4.8.6
Installation
path / port:       /phpmyadmin
```

Solution

Solution type: VendorFix

Update to version 4.8.6 or later.

Affected Software/OS

phpMyAdmin prior to version 4.8.6.

Vulnerability Insight

A vulnerability was reported where a specially crafted database name can be used to trigger an SQL injection attack through the designer feature.

Vulnerability Detection Method

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

Details: `phpMyAdmin < 4.8.6 SQL Injection Vulnerability - PMASA-2019-3 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.140207

Version used: `2019-06-11T04:26:53+0000`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.5.8`

Method: `phpMyAdmin Detection`

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2019-11768
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2019-3/
```

High (CVSS: 7.5)

NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.4.5
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108054

Version used: `$Revision: 11835 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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

High (CVSS: 7.5)

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809319
Version used: `$Revision: 11961 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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-2016-7124, 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 - 01 - Feb15

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

. . . continues on next page . . .

. . . continued from previous page . . .

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:5.4.5`
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 Out of Bounds Read Multiple Vulnerabilities - Jan15

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.37/5.5.21/5.6.5
```

Impact
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.

. . . continues on next page . . .

. . . continued from previous page . . .

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:5.4.5`
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 Arbitrary Code Execution Vulnerability - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

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 Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808671
Version used: `$Revision: 11903 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 7.5)
NVT: Drupal Third-party Libraries Vulnerability (SA-CORE-2019-007) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

Drupal is prone to a vulnerability in the 3rd party library Phar Stream Wrapper.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.67
Installation
path / port:       /drupal
```

Solution

Solution type: VendorFix
Update to version 7.67, 8.6.16, 8.7.1 or later.

Affected Software/OS

Drupal 7.x, 8.6.x or earlier and 8.7.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The vulnerability lies in third-party dependencies included in or required by Drupal core. As described in TYPO3-PSA-2019-007 (By-passing protection of Phar Stream Wrapper Interceptor).

Vulnerability Detection Method

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

Details: `Drupal Third-party Libraries Vulnerability (SA-CORE-2019-007) (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142385

Version used: `2019-05-14T07:15:16+0000`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2019-11831
Other:
  URL:https://www.drupal.org/sa-core-2019-007
   URL:https://typo3.org/security/advisory/typo3-psa-2019-007/
```

High (CVSS: 7.5)

NVT: Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Linux, Version Check)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to critical remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     Upgrade to 7.58
Installation
path / port:       /drupal
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code and completely compromise the site.

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to Drupal core version 8.3.9 or 8.4.6 or 8.5.1 or 7.58 or later. Please see the referenced links for available updates.

Affected Software/OS

Drupal core versions 6.x and earlier,
Drupal core versions 8.2.x and earlier,
Drupal core versions 8.3.x to before 8.3.9,
Drupal core versions 8.4.x to before 8.4.6,
Drupal core versions 8.5.x to before 8.5.1 and
Drupal core versions 7.x to before 7.58 on Linux.

Vulnerability Insight

The flaw exists within multiple subsystems of Drupal. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Li.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.812584
Version used: `$Revision: 12012 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2018-7600
Other:
  URL:https://www.drupal.org/psa-2018-001
   URL:https://www.drupal.org/sa-core-2018-002
   URL:https://www.drupal.org/project/drupal/releases/7.58
   URL:https://www.drupal.org/project/drupal/releases/8.3.9
   URL:https://www.drupal.org/project/drupal/releases/8.4.6
   URL:https://www.drupal.org/project/drupal/releases/8.5.1
   URL:https://research.checkpoint.com/uncovering-drupalgeddon-2/
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 5.6.25, or 7.0.10, or later.

Affected Software/OS

PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809317

Version used: `$Revision: 11938 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

`CVE: CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417,`

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪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 - 02 - Jan15

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     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 5.6.5 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:5.4.5`
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-2014-9426
Other:
  URL:https://bugs.php.net/bug.php?id=68665
   URL:http://securitytracker.com/id/1031480
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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.

Details: `PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808792

Version used: `$Revision: 12313 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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 - 01 - Jun15 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

. . . continues on next page . . .

... continued from previous page ...

- an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Jun15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805651
Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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 - 03 - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

... continues on next page ...

. . . continued from previous page . . .

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 Linux.

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.
- 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808603
Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jan15

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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:5.4.5`
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 Remote Code Execution Vulnerabilities - Jul15 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.805685

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807807
Version used: `$Revision: 12431 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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-2016-3142, 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: Drupal Multiple Vulnerabilities (SA-CORE-2019-001/SA-CORE-2019-002) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

Drupal is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.62
```

Solution

Solution type: VendorFix

Update to version 7.62, 8.5.9, 8.6.6 or later.

Affected Software/OS

Drupal 7.x, 8.5.x and 8.6.x.

Vulnerability Insight

Drupal is prone to multiple vulnerabilities:

- Drupal core uses the third-party PEAR Archive_Tar library. This library has released a security update which impacts some Drupal configurations. (CVE-2018-1000888)
- A remote code execution vulnerability exists in PHP's built-in phar stream wrapper when performing file operations on an untrusted phar:// URI.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Drupal Multiple Vulnerabilities (SA-CORE-2019-001/SA-CORE-2019-002) (Linux)`
OID:1.3.6.1.4.1.25623.1.0.141891
Version used: `$Revision: 13837 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2018-1000888, CVE-2019-6339, CVE-2019-6338
Other:
  URL:https://www.drupal.org/sa-core-2019-001
   URL:https://www.drupal.org/sa-core-2019-002
```

High (CVSS: 7.5)
NVT: Drupal Core SQL Injection Vulnerability

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary
Drupal is prone to an SQL-injection vulnerability

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

Impact
Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Solution
Solution type: VendorFix
Updates are available

Affected Software/OS
Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight
Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method
Send a special crafted HTTP POST request and check the response.
Details: `Drupal Core SQL Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105101
Version used: `$Revision: 13659 $`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2014-3704
BID:70595
Other:
  URL:http://www.securityfocus.com/bid/70595
   URL:http://drupal.org/
```

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.
This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://192.168.57.5/uploads/puttest292166886.html
We could delete the following files via the DELETE method at this web server:
http://192.168.57.5/uploads/puttest292166886.html
```

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution

Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method

Details: `Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `2019-04-24T07:26:10+0000`

References

```
BID:12141
Other:
  OWASP:OWASP-CM-001
```

High (CVSS: 7.8)
NVT: PHP Denial of Service Vulnerability Jul17 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.811487
Version used: `$Revision: 11874 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 8.5)
NVT: PHP Multiple Vulnerabilities - Dec18 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

Vulnerability Detection Method

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

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

OID:1.3.6.1.4.1.25623.1.0.108507

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

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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-2018-19396
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: 8.5)
NVT: Drupal Multiple Vulnerabilities02- May16 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.43
```

Impact

Successful exploitation will allow remote attackers to cause brute force attacks, to download and execute JSON-encoded content and also to gain elevated privileges.

Solution

Solution type: VendorFix

Upgrade to version 6.38 or 7.43 or later.

Affected Software/OS

Drupal 6.x before 6.38 and 7.x before 7.43 on Linux.

Vulnerability Insight

Multiple flaws exixts due to,
- An improper validation of JSON-encoded content in system module.
- The XML-RPC system allows a large number of calls to the same method.
- An error in 'user_save' function in User module.

Vulnerability Detection Method

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Drupal Multiple Vulnerabilities02- May16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808045
Version used: `2019-05-10T14:24:23+0000`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2016-3168, CVE-2016-3163, CVE-2016-3169
Other:
  URL:https://www.drupal.org/SA-CORE-2016-001
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method

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

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

OID:1.3.6.1.4.1.25623.1.0.807507

Version used: `$Revision: 12149 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 10.0)

NVT: PHP End Of Life Detection (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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:5.4.5
Installed version: 5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.105889
Version used: `$Revision: 12149 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 10.0)
NVT: phpMyAdmin End of Life Detection (Linux)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.5.8
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:3.5.8
Installed version: 3.5.8
Location/URL:      http://192.168.57.5/phpmyadmin
EOL version:       3.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.113015

Version used: `$Revision: 11982 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.5.8`

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/
```

High (CVSS: 10.0)

NVT: PHP Multiple Vulnerabilities - 03 - Jun15 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed Version:     5.4.40
```

Impact

. . . continues on next page . . .

... continued from previous page ...

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805657
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Product detection result
`cpe:/a:php:php:5.4.5`

... 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

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

Vulnerability Detection Result

```
Installed version: 5.4.5
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.

Affected Software/OS

PHP versions prior to 5.6.7 on Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808673

Version used: `$Revision: 14181 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 10.0)

NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808607
Version used: `$Revision: 12149 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 10.0)
NVT: Drupal Coder Remote Code Execution

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

The remote Drupal installation is prone to a remote code execution vulnerability.

Vulnerability Detection Result

```
Vulnerable url: http://192.168.57.5/drupal/sites/all/modules/coder/coder_upgrade
↪/scripts/coder_upgrade.run.php
```

Solution

Solution type: VendorFix
Install the latest version:

Vulnerability Insight

The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

Vulnerability Detection Method

Check for known error message from affected modules
Details: `Drupal Coder Remote Code Execution`
OID:1.3.6.1.4.1.25623.1.0.105818
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
Other:
  URL:https://www.drupal.org/node/2765575
```

[return to 192.168.57.5]

2.1.5 High 22/tcp

High (CVSS: 7.2)
NVT: OpenSSH Privilege Escalation Vulnerability - May16

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.2p2-3
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue will allow local users to gain privileges.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2p2-3 or later.

Affected Software/OS

OpenSSH versions through 7.2p2.

Vulnerability Insight

The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.

Vulnerability Detection Method

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

Details: `OpenSSH Privilege Escalation Vulnerability - May16`

OID:1.3.6.1.4.1.25623.1.0.807574

Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-8325
Other:
  URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4
↪e10a65c91810f88755
```

High (CVSS: 7.5)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.2
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2 or later.

Affected Software/OS

OpenSSH versions before 7.2 on Linux.

Vulnerability Insight

An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method

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

Details: `OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.810769

Version used: `2019-05-22T12:00:57+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`

Method: `OpenSSH Detection Consolidation`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-1908
BID:84427
Other:
  URL:http://openwall.com/lists/oss-security/2016/01/15/13
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
   URL:http://www.openssh.com/txt/release-7.2
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6f
↪a0db113c71e234416c
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741
```

High (CVSS: 7.5)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.4
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.4 or later.

Affected Software/OS

OpenSSH versions before 7.4 on Linux

Vulnerability Insight

Multiple flaws exists due to,

- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.

. . . continues on next page . . .

. . . continued from previous page . . .

- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.
- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.
- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Multiple Vulnerabilities Jan17 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.8103256
Version used: `2019-05-21T12:48:06+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10
↪708
BID:94968, 94972, 94977, 94975
Other:
  URL:https://www.openssh.com/txt/release-7.4
   URL:http://www.openwall.com/lists/oss-security/2016/12/19/2
   URL:http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e
↪933e6b931de1d16737
```

High (CVSS: 7.8)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.3
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

`path / port:        22/tcp`

Impact

Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.3 or later.

Affected Software/OS

OpenSSH versions before 7.3 on Linux

Vulnerability Insight

Multiple flaws exist due to,

- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.

- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method

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

Details: `OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809154

Version used: `2019-05-21T12:48:06+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-6515, CVE-2016-6210
BID:92212
Other:
  URL:http://www.openssh.com/txt/release-7.3
   URL:http://seclists.org/fulldisclosure/2016/Jul/51
   URL:https://security-tracker.debian.org/tracker/CVE-2016-6210
   URL:http://openwall.com/lists/oss-security/2016/08/01/2
```

High (CVSS: 8.5)

NVT: OpenSSH Multiple Vulnerabilities

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
This host is running OpenSSH and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.0
Installation
path / port:       22/tcp
```

Impact
Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.

Solution
Solution type: VendorFix
Upgrade to OpenSSH 7.0 or later.

Affected Software/OS
OpenSSH versions before 7.0.

Vulnerability Insight
Multiple flaws are due to:
- Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd.
- Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd.
- Vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.806052
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600
Other:
  URL:http://seclists.org/fulldisclosure/2015/Aug/54
   URL:http://openwall.com/lists/oss-security/2015/07/23/4
```

[return to 192.168.57.5]

2.1.6 Medium general/tcp

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Vulnerability Detection Result

```
Installed version: 2.4.7
Fixed version:     2.4.39
```

Solution

Solution type: VendorFix

Update to version 2.4.39 or later.

Affected Software/OS

Apache HTTP server version 2.4.38 and prior.

Vulnerability Detection Method

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

Details: `Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142228

Version used: `2019-06-17T06:50:08+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2019-0220
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.141964

Version used: `$Revision: 13750 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

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
```

Medium (CVSS: 6.0)
NVT: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
```

... continues on next page ...

. . . continued from previous page . . .

```
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Vulnerability Detection Result

```
Installed version: 2.4.7
Fixed version:     2.4.39
```

Solution

Solution type: VendorFix

Update to version 2.4.39 or later.

Affected Software/OS

Apache HTTP server version 2.4.38 and prior.

Vulnerability Detection Method

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

Details: `Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.142220

Version used: `2019-04-15T07:08:44+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2019-0217
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

[return to 192.168.57.5]

2.1.7 Medium 631/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`

OID:1.3.6.1.4.1.25623.1.0.108031

Version used: `$Revision: 5232 $`

References

```
CVE: CVE-2016-2183, CVE-2016-6329
Other:
  URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://sweet32.info/
```

[return to 192.168.57.5]

2.1.8 Medium 445/tcp

Medium (CVSS: 4.0)

NVT: Samba >= 4.0.0, <= 4.5.2 Privilege Escalation Vulnerability

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Samba is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.3.13
Installation
path / port:       445/tcp
```

Impact
Successful exploitation would allow an authenticated attacker to gain additional access rights.

Solution
Solution type: VendorFix
Update to version 4.3.13, 4.4.8 or 4.5.3 respectively.

Affected Software/OS
Samba versions 4.0.0 through 4.3.12, 4.4.0 through 4.4.7 and 4.5.0 through 4.5.2.

Vulnerability Insight
Samba is prone to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to creash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba >= 4.0.0, <= 4.5.2 Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113287
Version used: `$Revision: 12236 $`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2016-2126
BID:94994
Other:
  URL:https://www.samba.org/samba/security/CVE-2016-2126.html
```

Medium (CVSS: 4.0)
NVT: Samba 'AD LDAP' Information Disclosure Vulnerability - Aug18

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.6.16 or apply patch
Installation
path / port:       445/tcp
```

Impact

Successful exploitation will allow an attacker to gain access to confidential attribute values.

Solution

Solution type: VendorFix

Upgrade to Samba 4.8.4 or 4.7.9 or 4.6.16 or later. Please see the references for more information.

Affected Software/OS

All versions of Samba from 4.0.0 onwards

Vulnerability Insight

The flaw exists due to a missing access control checks.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba 'AD LDAP' Information Disclosure Vulnerability - Aug18`
OID:1.3.6.1.4.1.25623.1.0.813784
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-10919
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-10919.html
   URL:https://www.samba.org/samba/history/samba-4.8.4.html
   URL:https://www.samba.org/samba/history/samba-4.7.9.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:https://www.samba.org/samba/history/samba-4.6.16.html
```

Medium (CVSS: 4.0)
NVT: Samba DoS Vulnerability (CVE-2018-16841)

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

Samba is prone to a denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.7.12
Installation
path / port:       445/tcp
```

Solution

Solution type: VendorFix

Update to version 4.7.12, 4.8.7, 4.9.3 or later.

Affected Software/OS

Samba 4.3.0 and later.

Vulnerability Insight

A user with a valid certificate or smart card can crash the Samba AD DC's KDC.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba DoS Vulnerability (CVE-2018-16841)`
OID:1.3.6.1.4.1.25623.1.0.141734
Version used: `$Revision: 13517 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-16841
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-16841.html
```

Medium (CVSS: 4.0)
NVT: Samba 4.x Multiple DoS Vulnerabilities

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

Samba is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.7.12
Installation
path / port:       445/tcp
```

Solution

Solution type: VendorFix
Update to version 4.7.12, 4.8.7, 4.9.3 or later.

Affected Software/OS

Samba version 4.x.x.

Vulnerability Insight

Samba is prone to multiple vulnerabilities:
- CNAME loops can cause DNS server crashes, and CNAMEs can be added by unprivileged users. (CVE-2018-14629)
- A user able to read more than 256MB of LDAP entries can crash the Samba AD DC's LDAP server. (CVE-2018-16851)

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba 4.x Multiple DoS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.141732
Version used: `$Revision: 13517 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-14629, CVE-2018-16851
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-14629.html
   URL:https://www.samba.org/samba/security/CVE-2018-16851.html
```

Medium (CVSS: 4.8)
NVT: Samba Server 'SMB1' Memory Information Leak Vulnerability

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to memory information leak vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.4.16
Installation
path / port:       445/tcp
```

Impact

Successful exploitation will allow a client with write access to a share can cause server memory contents to be written into a file or printer.

Solution

Solution type: VendorFix

Upgrade to Samba 4.6.8, 4.5.14 and 4.4.16 or later.

Affected Software/OS

Samba versions before 4.4.16, 4.5.0 before 4.5.14, and 4.6.0 before 4.6.8.

Vulnerability Insight

A server memory information leak bug over SMB1 if a client can write data to a share. Some SMB1 write requests were not correctly range checked to ensure the client had sent enough data to fulfill the write.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba Server 'SMB1' Memory Information Leak Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.811905
Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-12163
BID:100925
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-12163.html
```

Medium (CVSS: 5.0)
NVT: Samba Server 'CVE-2017-15275' Heap Memory Information Leak

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to a heap memory information leak.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.5.15
Installation
path / port:       445/tcp
```

Impact

There is no known vulnerability associated with this error, but uncleared heap memory may contain previously used data that may help an attacker compromise the server via other methods. Uncleared heap memory may potentially contain password hashes or other high-value data.

Solution

Solution type: VendorFix

Update to Samba 4.5.15, 4.6.11, 4.7.3 or later.

Affected Software/OS

Samba versions 3.6.0 to 4.5.14, 4.6.x prior to 4.6.11, 4.7.x prior to 4.7.3.

Vulnerability Insight

The flaw exists due to the server which may return the contents of heap allocated memory to the client.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba Server 'CVE-2017-15275' Heap Memory Information Leak`
OID:1.3.6.1.4.1.25623.1.0.108295
Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2017-15275
BID:101908
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-15275.html
```

Medium (CVSS: 5.0)
NVT: Samba AD DC Principal Modification Vulnerability (CVE-2018-16860)

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

Samba is prone to a user impersonation vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.8.12
Installation
path / port:       445/tcp
```

Impact

This allows a man-in-the-middle attacker who can intercept the request to the KDC to modify the packet by replacing the user name (principal) in the request with any desired user name (principal) that exists in the KDC and replace the checksum protecting that name with a CRC32 checksum (which requires no prior knowledge to compute).

This would allow a S4U2Self ticket requested on behalf of user name (principal) user@EXAMPLE.COM to any service to be changed to a S4U2Self ticket with a user name (principal) of Administrator@EXAMPLE.COM. This ticket would then contain the PAC of the modified user name (principal).

Solution

Solution type: VendorFix

Update to version 4.8.12, 4.9.8, 4.10.3 or later.

Affected Software/OS

All Samba versions since Samba 4.0.

Vulnerability Insight

S4U2Self is an extension to Kerberos used in Active Directory to allow a service to request a kerberos ticket to itself from the Kerberos Key Distribution Center (KDC) for a non-Kerberos authenticated user (principal in Kerboros parlance). This is useful to allow internal code paths to be standardized around Kerberos.

. . . continues on next page . . .

... continued from previous page ...

S4U2Proxy (constrained-delegation) is an extension of this mechanism allowing this impersonation to a second service over the network. It allows a privileged server that obtained a S4U2Self ticket to itself to then assert the identity of that principal to a second service and present itself as that principal to get services from the second service.
There is a flaw in Samba's AD DC in the Heimdal KDC. When the Heimdal KDC checks the checksum that is placed on the S4U2Self packet by the server to protect the requested principal against modification, it does not confirm that the checksum algorithm that protects the user name (principal) in the request is keyed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba AD DC Principal Modification Vulnerability (CVE-2018-16860)`
OID:1.3.6.1.4.1.25623.1.0.108575
Version used: `2019-05-16T10:55:33+0000`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-16860
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-16860.html
```

Medium (CVSS: 5.5)
NVT: Samba Path/Symlink Traversal Vulnerability (CVE-2019-3880)

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary
Samba is prone to a path/symlink traversal vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.8.11
Installation
path / port:       445/tcp
```

Solution
Solution type: VendorFix
Update to version 4.8.11, 4.9.6, 4.10.2 or later.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
Samba 3.2.0 and later.

Vulnerability Insight
A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba Path/Symlink Traversal Vulnerability (CVE-2019-3880)`
OID:1.3.6.1.4.1.25623.1.0.142391
Version used: `2019-05-09T14:21:05+0000`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
```
CVE: CVE-2019-3880
Other:
  URL:https://www.samba.org/samba/security/CVE-2019-3880.html
```

Medium (CVSS: 5.8)
NVT: Samba Server 'SMB 1/2/3' MitM Vulnerability

Product detection result
```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary
This host is running Samba and is prone to MitM vulnerability.

Vulnerability Detection Result
```
Installed version: 4.3.11
Fixed version:     4.4.16, or 4.5.14, or 4.6.8
Installation
path / port:       445/tcp
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow a remote attacker to read and/or alter the content of the connection.

Solution
Solution type: VendorFix
Upgrade to Samba 4.6.8, 4.5.14 or 4.4.16

Affected Software/OS
Samba versions 3.0.25 to 4.6.7

Vulnerability Insight
The flaw exists due to there are several code paths where the code doesn't enforce SMB signing.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba Server 'SMB 1/2/3' MitM Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.811907
Version used: `$Revision: 11983 $`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-12150
BID:100918
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-12150.html
```

Medium (CVSS: 6.5)
NVT: Samba 4 Multiple Vulnerabilities

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary
Multiple Vulnerabilities in Samba 4.0 onward.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.5.16
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

`path / port:        445/tcp`

Impact

Successful exploitation would result in effects ranging from Denial of Service to Privilege Escalation, eventually allowing an attacker to gain full control over the target system.

Solution

Solution type: VendorFix

Update to Samba version 4.5.16, 4.6.14 or 4.7.6 respectively.

Affected Software/OS

Samba 4.x.x before 4.5.16, 4.6.x before 4.6.14 and 4.7.x before 4.7.6.

Vulnerability Insight

There exist two vulnerabilities:

- Samba is vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.
- On a Samba AD DC the LDAP server in Samba incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).

Vulnerability Detection Method

The script checks if a vulnerable version is present on the target host.

Details: `Samba 4 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.113133

Version used: `$Revision: 12120 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`

Method: `SMB NativeLanMan`

OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-1050, CVE-2018-1057
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-1050.html
   URL:https://www.samba.org/samba/security/CVE-2018-1057.html
```

Medium (CVSS: 6.5)

NVT: Samba 'libsmbclient' Heap Buffer Overflow Vulnerability - Aug18

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is running Samba and is prone to a heap based buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.6.16 or apply patch
Installation
path / port:       445/tcp
```

Impact

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

Solution

Solution type: VendorFix

Upgrade to Samba 4.6.16, 4.7.9 or 4.8.4 or later. Please see the references for more information.

Affected Software/OS

Samba versions 3.2.0 through 4.8.3

Vulnerability Insight

The flaw exists due to insufficient input validation on client directory listing in libsmbclient.

Vulnerability Detection Method

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

Details: `Samba 'libsmbclient' Heap Buffer Overflow Vulnerability - Aug18`

OID:1.3.6.1.4.1.25623.1.0.813782

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`

Method: `SMB NativeLanMan`

OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2018-10858
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-10858.html
   URL:https://www.samba.org/samba/history/samba-4.6.16.html
   URL:https://www.samba.org/samba/history/samba-4.7.9.html
   URL:https://www.samba.org/samba/history/samba-4.8.4.html
```

Medium (CVSS: 6.8)

NVT: Samba Badlock Critical Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to badlock vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.2.11 or 4.3.8 or 4.4.2, or later
Installation
path / port:       445/tcp
```

Impact

Successful exploitation of this vulnerability leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spoof and to obtain sensitive session information.

Solution

Solution type: VendorFix

Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later.

Affected Software/OS

Samba versions 3.0.x through 4.4.1

- —-

NOTE: Samba versions 4.2.11, 4.3.8 are not affected

- —-

Vulnerability Insight

The multiple flaws are due to,

- The Multiple errors in DCE-RPC code.
- A spoofing Vulnerability in NETLOGON.
- The LDAP implementation did not enforce integrity protection for LDAP connections.
- The SSL/TLS certificates are not validated in certain connections.
- Not enforcing Server Message Block (SMB) signing for clients using the SMB1 protocol.
- An integrity protection for IPC traffic is not enabled by default
- The MS-SAMR and MS-LSAD protocol implementations mishandle DCERPC connections.
- An error in the implementation of NTLMSSP authentication.

Vulnerability Detection Method

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

Details: `Samba Badlock Critical Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.807646

Version used: `$Revision: 11772 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2016-2118, CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112,
↪CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-0128
Other:
  URL:http://badlock.org/
   URL:http://thehackernews.com/2016/03/windows-samba-vulnerability.html
```

Medium (CVSS: 6.8)
NVT: Samba Man in the Middle Security Bypass Vulnerability (Heimdal)

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to a MITM authentication validation bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.4.15
Installation
path / port:       445/tcp
```

Impact

Successfully exploiting this issue will allow a MITM attacker to impersonate a trusted server and thus gain elevated access to the domain by returning malicious replication or authorization data.

Solution

Solution type: VendorFix
Upgrade to Samba 4.6.6 or 4.5.12 or 4.4.15 or later or apply the patch from below.

Affected Software/OS

All versions of Samba from 4.0.0 before 4.6.6 or 4.5.12 or 4.4.15.
Note: All versions of Samba from 4.0.0 onwards using embedded Heimdal Kerberos. Samba binaries built against MIT Kerberos are not vulnerable.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The flaw is due to error in function '_krb5_extract_ticket' where the KDC-REP service name must be obtained from encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unecrypted version provides an opportunity for successful server impersonation and other attacks.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Samba Man in the Middle Security Bypass Vulnerability (Heimdal)`
OID:1.3.6.1.4.1.25623.1.0.811522
Version used: `$Revision: 11901 $`

Product Detection Result

Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-11103
BID:99551
Other:
  URL:https://www.samba.org/samba/security/CVE-2017-11103.html
   URL:https://www.samba.org/samba/security
```

Medium (CVSS: 6.8)
NVT: Samba 'fd_open_atomic infinite loop' Denial-of-Service Vulnerability

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

This host is running Samba and is prone to denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.4.10
Installation
path / port:       445/tcp
```

Impact

Successfully exploiting this issue will allow remote attackers to conduct a denial-of-service condition(infinite loop with high CPU usage and memory consumption).

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to Samba 4.4.10 or 4.5.6 or later.

Affected Software/OS
Samba versions before 4.4.10 and 4.5.x before 4.5.6

Vulnerability Insight
The flaw exists due to error in smbd which enters infinite loop when trying to open an invalid symlink with O_CREAT.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba 'fd_open_atomic infinite loop' Denial-of-Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.811083
Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2017-9461
Other:
  URL:https://bugzilla.samba.org/show_bug.cgi?id=12572
   URL:https://git.samba.org/?p=samba.git;a=commit;h=10c3e3923022485c720f322ca4f
↪0aca5d7501310
```

[return to 192.168.57.5]

2.1.9 Medium 3500/tcp

Medium (CVSS: 5.0)
NVT: Ruby on Rails Acrive Model Security Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:ruby-lang:ruby:2.3.7
Detected by Ruby on Rails Version Detection (OID: 1.3.6.1.4.1.25623.1.0.902089)
```

Summary
This host is running Ruby on Rails and is prone to security bypass vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.2.4
Fixed version:     4.2.5.1
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow a remote attacker to bypass intended change restrictions by leveraging use of the nested attributes feature.

Solution
Solution type: VendorFix
Upgrade to Ruby on Rails 4.1.14.1 or 4.2.5.1, or later.

Affected Software/OS
Ruby on Rails 4.1.x before 4.1.14.1, Ruby on Rails 4.2.x before 4.2.5.1 on Linux.

Vulnerability Insight
The flaw is due to Ruby on Rails supports the use of instance-level writers for class accessors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Acrive Model Security Bypass Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809361
Version used: `2019-07-05T10:16:38+0000`

Product Detection Result
Product: `cpe:/a:ruby-lang:ruby:2.3.7`
Method: `Ruby on Rails Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.902089)

References

```
CVE: CVE-2016-0753
BID:82247
Other:
  URL:http://www.openwall.com/lists/oss-security/2016/01/25/14
```

Medium (CVSS: 5.0)
NVT: Ruby on Rails Active Record SQL Injection Vulnerability (Linux)

Product detection result

```
cpe:/a:ruby-lang:ruby:2.3.7
Detected by Ruby on Rails Version Detection (OID: 1.3.6.1.4.1.25623.1.0.902089)
```

Summary
This host is running Ruby on Rails and is prone to SQL injection vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.4
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     4.2.7.1
```

Impact

Successful exploitation will allow a remote attacker to bypass intended database-query restrictions and perform NULL checks or trigger missing WHERE clauses via a crafted request, as demonstrated by certain '[nil]' values.

Solution

Solution type: VendorFix

Upgrade to Ruby on Rails 4.2.7.1 or later.

Affected Software/OS

Ruby on Rails 4.2.x before 4.2.7.1 on Linux

Vulnerability Insight

The flaw is due to the way Active Record interprets parameters in combination with the way that JSON parameters are parsed, it is possible for an attacker to issue unexpected database queries with 'IS NULL' or empty where clauses.

Vulnerability Detection Method

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

Details: `Ruby on Rails Active Record SQL Injection Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.807378

Version used: `2019-07-05T10:16:38+0000`

Product Detection Result

Product: `cpe:/a:ruby-lang:ruby:2.3.7`

Method: `Ruby on Rails Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.902089)

References

```
CVE: CVE-2016-6317
BID:92434
Other:
  URL:http://www.openwall.com/lists/oss-security/2016/08/11/4
   URL:https://groups.google.com/forum/#!topic/ruby-security-ann/WccgKSKiPZA
   URL:http://weblog.rubyonrails.org/2016/8/11/Rails-5-0-0-1-4-2-7-2-and-3-2-22-
↪3-have-been-released
```

Medium (CVSS: 5.0)

NVT: Ruby on Rails Action Pack Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:ruby-lang:ruby:2.3.7
Detected by Ruby on Rails Version Detection (OID: 1.3.6.1.4.1.25623.1.0.902089)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running Ruby on Rails and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2.4
Fixed version:     4.2.5.1
```

Impact
Successful exploitation will allow a remote attacker to cause a denial of service condition.

Solution
Solution type: VendorFix
Upgrade to Ruby on Rails 4.2.5.1, or later.

Affected Software/OS
Ruby on Rails 4.x before 4.2.5.1 on Linux.

Vulnerability Insight
The flaw is due to an error in 'actionpack/lib/action_dispatch/routing/route_set.rb' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Action Pack Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809363
Version used: `2019-07-05T10:16:38+0000`

Product Detection Result
Product: `cpe:/a:ruby-lang:ruby:2.3.7`
Method: `Ruby on Rails Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.902089)

References

```
CVE: CVE-2015-7581
BID:81677
Other:
  URL:http://www.openwall.com/lists/oss-security/2016/01/25/14
```

[return to 192.168.57.5]

2.1.10 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Anonymous sessions:     331 Anonymous login ok, send your complete email address
↪ as your password
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `$Revision: 13611 $`

[return to 192.168.57.5]

2.1.11 Medium 80/tcp

Medium (CVSS: 4.3)
NVT: Apache HTTP Server Mod_Cache Denial of service Vulnerability -01 May15

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
Fixed version:     2.4.10
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow a remote attackers to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution

Solution type: VendorFix

Upgrade to version 2.4.10 or later.

Affected Software/OS

Apache HTTP Server version 2.4.6 through 2.4.9.

Vulnerability Insight

Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server.

Vulnerability Detection Method

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

Details: `Apache HTTP Server Mod_Cache Denial of service Vulnerability -01 May15`

OID:1.3.6.1.4.1.25623.1.0.805635

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2014-0117
BID:68740
Other:
  URL:http://zerodayinitiative.com/advisories/ZDI-14-239/
   URL:http://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 4.3)

NVT: phpMyAdmin < 4.9.0 CSRF Vulnerability - PMASA-2019-4 (Linux)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.5.8
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

phpMyAdmin is prone to a CSRF vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 3.5.8
Fixed version:     4.9.0
Installation
path / port:       /phpmyadmin
```

Solution

Solution type: VendorFix
Update to version 4.9.0 or later.

Affected Software/OS

phpMyAdmin prior to version 4.9.0.

Vulnerability Insight

A vulnerability was found that allows an attacker to trigger a CSRF attack against a phpMyAdmin user. The attacker can trick the user, for instance through a broken <img> tag pointing at the victim's phpMyAdmin database, and the attacker can potentially deliver a payload (such as a specific INSERT or DELETE statement) through the victim.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `phpMyAdmin < 4.9.0 CSRF Vulnerability - PMASA-2019-4 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142499
Version used: `2019-06-11T04:26:53+0000`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.5.8`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2019-12616
Other:
  URL:https://www.phpmyadmin.net/security/PMASA-2019-4/
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Linux)

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.5.8
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 3.5.8
Fixed version:     4.8.3
```

Solution

Solution type: VendorFix

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.113255

Version used: `$Revision: 12164 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.5.8`

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: Drupal jQuery XSS Vulnerability (SA-CORE-2019-006) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

Drupal is prone to a cross-site scripting vulnerability in jQuery.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.66
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /drupal
```

Solution

Solution type: VendorFix

Update to version 7.66, 8.5.15, 8.6.15 or later.

Affected Software/OS

Drupal 7, 8.5.x or earlier and 8.6.x.

Vulnerability Insight

jQuery 3.4.0 includes a fix for some unintended behavior when using jQuery.extend(true, }}, ...). If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype. This fix is included in jQuery 3.4.0, but patch diffs exist to patch previous jQuery versions.

Vulnerability Detection Method

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

Details: `Drupal jQuery XSS Vulnerability (SA-CORE-2019-006) (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142300

Version used: `2019-04-24T09:29:51+0000`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2019-11358
Other:
  URL:https://www.drupal.org/sa-core-2019-006
```

Medium (CVSS: 4.3)

NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

Product detection result

```
cpe:/a:php:php:5.4.5
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 information disclosure vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      5.3.22/5.4.12
```

Impact

Successful exploitation will allow remote attackers to obtain sensitive information.

Solution

Solution type: VendorFix

Upgrade to PHP 5.3.22 or 5.4.12 or later.

Affected Software/OS

PHP version before 5.3.22 and 5.4.x before 5.4.12

Vulnerability Insight

Flaws are due to the way SOAP parser process certain SOAP objects (due to allowed expansion of XML external entities during SOAP WSDL files parsing).

Vulnerability Detection Method

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

Details: `PHP SOAP Parser Multiple Information Disclosure Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.803764

Version used: `$Revision: 11883 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2013-1824
BID:62373
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://www.php.net/downloads.php
   URL:http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530
↪acb8283c3bf4
```

Medium (CVSS: 4.3)

NVT: phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Linux

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.5.8
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is installed with phpMyAdmin and is prone to cross site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 3.5.8
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.

Solution

Solution type: VendorFix

Upgrade to version 4.8.2 or newer. Please see the references for more information.

Affected Software/OS

phpMyAdmin versions prior to 4.8.2 on Linux

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)-Linux`

OID:1.3.6.1.4.1.25623.1.0.813451

Version used: `2019-05-17T10:45:27+0000`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.5.8`

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: 4.3)

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

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:php:php:5.4.5
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

```
Installed version: 5.4.5
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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812735
Version used: `$Revision: 12120 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 4.3)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809137
Version used: `$Revision: 14181 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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-2015-8935
BID:92356
Other:
  URL:https://bugs.php.net/bug.php?id=68978
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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: `2019-07-05T09:54:18+0000`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:apache:http_server:2.4.7`
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
```

Medium (CVSS: 4.3)
NVT: PHP 'LibGD' Denial of Service Vulnerability

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.32/5.5.16/5.6.0
```

Impact

Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.

Affected Software/OS

PHP version 5.x through 5.4.26 and probably other versions.

Vulnerability Insight

The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'LibGD' Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.804292
Version used: `$Revision: 11867 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-2497
BID:66233
Other:
  URL:https://bugs.php.net/bug.php?id=66901
   URL:http://php.net
```

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.57.5/drupal/:pass
http://192.168.57.5/drupal/?D=A:pass
http://192.168.57.5/payroll_app.php:password
http://192.168.57.5/phpmyadmin/:pma_password
http://192.168.57.5/phpmyadmin/?D=A:pma_password
http://192.168.57.5/phpmyadmin/index.php:pma_password
http://192.168.57.5/phpmyadmin/license.php:pma_password
http://192.168.57.5/phpmyadmin/url.php:pma_password
```

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)
OID:1.3.6.1.4.1.25623.1.0.812512
Version used: $Revision: 12120 $

Product Detection Result

Product: cpe:/a:php:php:5.4.5
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 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

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
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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108505
Version used: `$Revision: 12938 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
Fixed version:     2.4.28
```

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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:2.4.7`
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: 5.0)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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. Please see the references for more information.

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 Linux.

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812849
Version used: `2019-05-03T08:55:39+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2018-1303
BID:103522
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 5.0)
NVT: Drupal Multiple Vulnerabilities Dec16 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.52
```

Impact

Successful exploitation will allow remote attackers to cause a denial of service condition, obtain sensitive information, conduct cache poisoning attacks and conduct open redirect attacks.

Solution

Solution type: VendorFix

Upgrade to version 7.52 or 8.2.3 or newer.

Affected Software/OS

Drupal core 7.x versions prior to 7.52 and 8.x versions prior to 8.2.3 on Linux

Vulnerability Insight

Multiple flaws are due to,

- An inconsistent naming of access query tags for taxonomy terms.
- The user password reset form does not specify a proper cache context.
- The confirmation forms allow external URLs to be injected.
- An error in transliterate mechanism.

Vulnerability Detection Method

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

Details: `Drupal Multiple Vulnerabilities Dec16 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.810224

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452
BID:94367
Other:
  URL:https://www.drupal.org/SA-CORE-2016-005
```

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://192.168.57.5/
http://192.168.57.5/drupal/misc
http://192.168.57.5/drupal/misc/farbtastic
http://192.168.57.5/drupal/misc/ui
http://192.168.57.5/drupal/sites/default/files
http://192.168.57.5/uploads
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.

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: PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14

Product detection result

```
cpe:/a:php:php:5.4.5
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 vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.5
Fixed version:     5.4.29/5.5.13
```

Impact

Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution

Solution type: VendorFix
Upgrade to PHP version 5.4.29 or 5.5.13 or later.

Affected Software/OS

PHP version 5.x before 5.4.29 and 5.5.x before 5.5.13

Vulnerability Insight

The flaw is due to
- An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script.
- An error within the 'cdf_read_property_info' function in src/cdf.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14`
OID:1.3.6.1.4.1.25623.1.0.804639
Version used: `$Revision: 11867 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-0237, CVE-2014-0238
BID:67759, 67765
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://secunia.com/advisories/58804
```

... continues on next page ...

. . . continued from previous page . . .

```
URL:https://www.hkcert.org/my_url/en/alert/14060401
URL:http://php.net
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.6.30
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overread 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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108052

Version used: `$Revision: 11863 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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-2016-10161, CVE-2016-10158
Other:
  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 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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. Please see the references for more information.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (L.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.813901
Version used: `2019-05-13T06:06:12+0000`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: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: 5.0)
NVT: Apache HTTP Server Multiple Vulnerabilities August15 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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 linux.

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.806018

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

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: PHP Multiple Vulnerabilities - Jul17 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.6.31
```

Impact

Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.811482
Version used: `$Revision: 11900 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 5.0)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
Installed version: 5.4.5
Fixed version:     5.6.0
```

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 Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808669

Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 5.0)

NVT: Drupal Password Hashing Denial of Service Vulnerability

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

A vulnerability in the password hashing API of Drupal 7 can lead to a DoS.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.34
```

Impact

An unauthenticated attacker can cause a denial of service.

Solution

Solution type: VendorFix

Upgrade to Drupal 7.34 or later.

Affected Software/OS

Drupal 7 before 7.34.

Vulnerability Insight

Drupal 7 includes a password hashing API to ensure that user supplied passwords are not stored in plain text. An attacker can send specially crafted requests resulting in CPU and memory exhaustion.

Vulnerability Detection Method

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

Details: `Drupal Password Hashing Denial of Service Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.105934

Version used: `$Revision: 14033 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2014-9016
BID:71202
Other:
  URL:https://www.drupal.org/SA-CORE-2014-006
   URL:http://www.behindthefirewalls.com/2014/12/cve-2014-9016-and-cve-2014-9034
↪-PoC.html
```

Medium (CVSS: 5.0)

NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15

Product detection result

```
cpe:/a:apache:http_server:2.4.7
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 2.4.7
Fixed version:     2.4.13
```

Impact
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: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.7`
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
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

Affected Software/OS

PHP versions prior to 5.6.12 on Linux

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 Multiple Denial of Service Vulnerabilities (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808611

Version used: `$Revision: 11961 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 5.0)
NVT: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

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 - (Linux)`
OID:1.3.6.1.4.1.25623.1.0.811490
Version used: `$Revision: 11982 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 5.0)
NVT: PHP 'URL checks' Security Bypass Vulnerability Jul17 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.811489
Version used: `$Revision: 11874 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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 'open_basedir' Security Bypass Vulnerability

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     N/A
```

Impact

Successful exploitation will allow remote attackers to read arbitrary files.

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

PHP versions 5.x.0 to 5.0.5, 5.1.0 to 5.1.6, 5.2.0 to 5.2.17, 5.3.0 to 5.3.27, 5.4.0 to 5.4.23 and 5.5.0 to 5.5.6.

Vulnerability Insight

The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'open_basedir' Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.804241
Version used: `$Revision: 11867 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2012-1171
Other:
  URL:https://bugzilla.redhat.com/show_bug.cgi?id=802591
```

Medium (CVSS: 5.0)
NVT: PHP 'donate' function Denial of Service Vulnerability - Nov14

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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

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:5.4.5`
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 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812073
Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2017-16642
BID:101745
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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.
Details: `Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812033
Version used: `$Revision: 11983 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`
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 'mod_auth_digest' DoS Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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 Linux.

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812067

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2019-05-17T13:14:58+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

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

Medium (CVSS: 5.0)
NVT: Drupal Information Disclosure Vulnerability

Summary

The host is running Drupal and is prone to information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable url: http://192.168.57.5/drupal/modules/simpletest/tests/upgrade/drup
↪al-6.upload.database.php
```

Impact

Successful exploitation will allow attacker to obtain sensitive information that could aid in further attacks.

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

Drupal Version 7.0.

Vulnerability Insight

The flaw is due to insufficient error checking, allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message.

Vulnerability Detection Method

Details: `Drupal Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902574
Version used: `2019-05-14T12:12:41+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2011-3730
Other:
  URL:http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/!_README
   URL:http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/drupal-7
↪.0
```

Medium (CVSS: 5.1)
NVT: Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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.

Affected Software/OS

Apache HTTP Server through 2.4.23 on Linux

- — 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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808632

Version used: `2019-07-05T09:54:18+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.7`
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
```

Medium (CVSS: 5.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.6.24/7.0.9
```

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 Linux

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808628
Version used: `$Revision: 11969 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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: 5.1)
NVT: PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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-based buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.5
Fixed version:     5.4.30
```

Impact

Successfully exploiting this issue allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code on the affected system.

Solution

Solution type: VendorFix
Update to PHP version 5.6.0 or 5.5.14 or 5.4.30 or 5.3.29 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

PHP versions 5.6.x alpha and beta releases before 5.6.0, 5.5.x before 5.5.14, 5.4.x before 5.4.30, 5.3.x before 5.3.29 on Linux

Vulnerability Insight

The flaw is due to buffer overflow error in the 'php_parserr' function in ext/standard/dns.c script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809743
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-4049
BID:68007
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://www.openwall.com/lists/oss-security/2014/06/13/4
   URL:http://www.php.net
```

Medium (CVSS: 5.8)
NVT: Drupal Multiple Vulnerabilities - March16 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.43
```

Impact

Successful exploitation will allow remote attackers to conduct open redirect attack.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Upgrade to version 6.38 or 7.43 or 8.0.4 later.

Affected Software/OS
Drupal 6.x before 6.38, 7.x before 7.43 and 8.X before 8.0.4 on Linux.

Vulnerability Insight
The flaw exists due to the current path being populated with an external URL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Drupal Multiple Vulnerabilities - March16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807481
Version used: `2019-05-16T08:02:32+0000`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2016-3164
Other:
  URL:https://www.drupal.org/SA-CORE-2016-001
```

Medium (CVSS: 5.8)
NVT: Drupal Core Multiple Vulnerabilities (SA-CORE-2015-001) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary
This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.35
```

Impact
Successful exploitation will allow remote attackers to gain access to another user's account without knowing the account's password and also trick users into being redirected to a 3rd party website, thereby exposing the users to potential social engineering attacks.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to Drupal core version 6.35 or 7.35 or later.

Affected Software/OS

Drupal core 6.x versions prior to 6.35 and 7.x versions prior to 7.35 on Linux.

Vulnerability Insight

Multiple flaws are due to,

- An improper validation for 'destination' query string parameter in URLs to redirect users to a new destination after completing an action on the current page.
- An improper implementation of several URL-related API functions.
- An improper handling of Password reset URLs.

Vulnerability Detection Method

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

Details: `Drupal Core Multiple Vulnerabilities (SA-CORE-2015-001) (Linux)`

OID:1.3.6.1.4.1.25623.1.0.811831

Version used: `$Revision: 11983 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2015-2750, CVE-2015-2749, CVE-2015-2559
BID:73219, 73403, 73219
Other:
  URL:https://www.drupal.org/SA-CORE-2015-001
```

Medium (CVSS: 6.4)

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.6.30
```

. . . continues on next page . . .

. . . continued from previous page . . .

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 - (Linux)`

OID:1.3.6.1.4.1.25623.1.0.811484

Version used: `$Revision: 11863 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 6.4)

NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.4.5
Fixed version:     5.5.31
```

Impact

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 Linux.

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.809139

Version used: `$Revision: 12051 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 6.4)

NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.5
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 Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.807504

Version used: `$Revision: 12338 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 6.4)

NVT: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
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 Linux.

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.811237
Version used: `$Revision: 14173 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.7`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

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
```

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

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
Fixed version:     5.4.44
```

Impact

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 Linux

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808666
Version used: `$Revision: 12051 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Medium (CVSS: 6.5)
NVT: Drupal 'User' Module Privilege Escalation Vulnerability (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.44
```

Impact

Successful exploitation will allow remote attackers to gain access to administrative privileges.

Solution

Solution type: VendorFix

Upgrade to version 7.44 or newer.

Affected Software/OS

Drupal core 7.x versions prior to 7.44

Vulnerability Insight

The Flaw exists due to error within the 'User' module, where a specific code can trigger a rebuild of the user profile form and a registered user can be granted all user roles on the site.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Drupal 'User' Module Privilege Escalation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807885
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2016-6211
BID:91230
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:https://www.drupal.org/SA-CORE-2016-002
```

Medium (CVSS: 6.5)
NVT: Drupal Multiple Vulnerabilities03- May16 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.43
```

Impact

Successful exploitation will allows remote attackers to cause information disclosure, bypass access restrictions and read, delete, or substitute a link to a file.

Solution

Solution type: VendorFix

Upgrade to version 7.43 or 8.0.4 or later.

Affected Software/OS

Drupal 7.x before 7.43 and 8.x before 8.0.4 on Linux.

Vulnerability Insight

Multiple flaws exixts due to,

- An email address can be matched to an account.
- An improper validation of File module.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Drupal Multiple Vulnerabilities03- May16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808047
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2016-3170, CVE-2016-3162
Other:
  URL:https://www.drupal.org/SA-CORE-2016-001
```

Medium (CVSS: 6.8)
NVT: Apache HTTP Server Multiple Vulnerabilities May15

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
Fixed version:     2.4.10
```

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 2.4.10 or later.

Affected Software/OS

Apache HTTP Server version before 2.4.10.

Vulnerability Insight

Multiple flaws are due to:
- Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used.
- Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies.
- A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard.
- Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Multiple Vulnerabilities May15`
OID:1.3.6.1.4.1.25623.1.0.805638

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2019-07-05T09:54:18+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.7`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2014-3523, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231
BID:73040
Other:
  URL:http://httpd.apache.org/security/vulnerabilities_24.html
   URL:http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109
```

Medium (CVSS: 6.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

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 Linux

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

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808609
Version used: `$Revision: 12313 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 6.8)
NVT: PHP Multiple Vulnerabilities - 01 - Aug14

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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,

. . . continues on next page . . .

. . . continued from previous page . . .

- Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script.
- 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:5.4.5`
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: Drupal Core Multiple Security Vulnerabilities (SA-CORE-2018-006) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.60
Installation
path / port:       /drupal
```

Solution

Solution type: VendorFix
Upgrade to Drupal core version 7.60, 8.5.8 or 8.6.2 respectively.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Drupal core versions 7.x before 7.60, 8.5.x before 8.5.8 and 8.6.x before 8.6.2 on Linux.

Vulnerability Insight
Drupal is prone to the following vulnerabilities:
- In some conditions, content moderation fails to check a users access to use certain transitions, leading to an access bypass.
- The path module allows users with the 'administer paths' to create pretty URLs for content. In certain circumstances the user can enter a particular path that triggers an open redirect to a malicious url.
- Drupal core and contributed modules frequently use a 'destination' query string parameter in URLs to redirect users to a new destination after completing an action on the current page. Under certain circumstances, malicious users can use this parameter to construct a URL that will trick users into being redirected to a 3rd party website, thereby exposing the users to potential social engineering attacks.
- When sending email some variables were not being sanitized for shell arguments, which could lead to remote code execution.
- The Contextual Links module doesn't sufficiently validate the requested contextual links. This vulnerability is mitigated by the fact that an attacker must have a role with the permission 'access contextual links'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Drupal Core Multiple Security Vulnerabilities (SA-CORE-2018-006) (Linux)`
OID:1.3.6.1.4.1.25623.1.0.112394
Version used: `$Revision: 12041 $`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References
```
Other:
  URL:https://www.drupal.org/SA-CORE-2018-006
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

Product detection result
```
cpe:/a:php:php:5.4.5
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
Installed Version: 5.4.5
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.806649

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

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: 6.8)
NVT: Drupal Session Hijacking Vulnerability

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary
Drupal is vulnerable to session hijacking.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.34
```

Impact
An attacker may gain unauthorized access to the application.

Solution
Solution type: VendorFix
Upgrade to Drupal 6.34, 7.34 or later.

Affected Software/OS
Drupal 6.x versions prior to 6.34. Drupal 7.x versions prior to 7.34.

Vulnerability Insight
A special crafted request can give a user access to another user's session, allowing an attacker to hijack a random session.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Drupal Session Hijacking Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105935
Version used: `$Revision: 14033 $`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2014-9015
BID:71195
Other:
  URL:https://www.drupal.org/SA-CORE-2014-006
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities May18 (Linux)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.5
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 multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.4.5
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. Please see the references for more information.

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 Linux.

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813160
Version used: `2019-05-03T08:55:39+0000`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

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: 6.8)
NVT: PHP 'PHP-FPM' Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP 'PHP-FPM' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812520
Version used: `$Revision: 12762 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2015-9253
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: 6.8)
NVT: Drupal Multiple Vulnerabilities - August15 (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.39
```

Impact

Successful exploitation will allow remote attackers to gain access to sensitive information, execute arbitrary HTML and script code in a user's browser session in the context of an affected site and conduct CSRF attacks.

Solution

Solution type: VendorFix
Upgrade to version 6.37 or 7.39 later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Drupal 6.x before 6.37 and 7.x before 7.39 on Linux.

Vulnerability Insight

Multiple flaws exixts as,

- The Form API in the application does not properly validate the form token.
- There is no restriction to get node titles by reading the menu.
- Insufficient sanitization of user-supplied input.

Vulnerability Detection Method

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

Details: `Drupal Multiple Vulnerabilities - August15 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.805965

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`

Method: `Drupal Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2015-6661, CVE-2015-6660, CVE-2015-6658
Other:
  URL:https://www.drupal.org/SA-CORE-2015-003
```

Medium (CVSS: 6.8)

NVT: PHP Multiple Vulnerabilities - 04 - Jun15 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805658
Version used: `$Revision: 12986 $`

Product Detection Result
Product: `cpe:/a:php:php:5.4.5`
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: 6.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.7
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: 2.4.7
Fixed version:     2.4.30
Installation
path / port:       80/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

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. Please see the references for more information.

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 Linux.

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.812844

Version used: `2019-05-03T08:55:39+0000`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.7`

Method: `Apache Web Server Detection`

OID: 1.3.6.1.4.1.25623.1.0.900498)

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: 6.8)

NVT: Drupal Core Multiple Vulnerabilities (SA-CORE-2018-001) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running Drupal and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.57
Installation
path / port:       /drupal
```

Impact
Successful exploitation will allow remote attackers to trick users into unwillingly navigating to an external site, update certain data that they do not have the permissions for, execute arbitrary script and gain extra privileges.

Solution
Solution type: VendorFix
Upgrade to Drupal core version 8.4.5 or 7.57 or later.

Affected Software/OS
Drupal core version 8.x versions prior to 8.4.5 and 7.x versions prior to 7.57 on Linux.

Vulnerability Insight
Multiple flaws are due to,
- An improper access restriction for sensitive contents via 'Comment reply form'.
- 'Drupal.checkPlain' JavaScript function does not correctly handle all methods of injecting malicious HTML.
- Private file access check fails under certain conditions in which one module is trying to grant access to the file and another is trying to deny it.
- A jQuery cross site scripting vulnerability is present when making Ajax requests to untrusted domains.
- Language fallback can be incorrect on multilingual sites with node access restrictions.
- An error in 'Settings Tray module'.
- An external link injection vulnerability when the language switcher block is used.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Drupal Core Multiple Vulnerabilities (SA-CORE-2018-001) (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812776
Version used: `$Revision: 12012 $`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6930,
↪CVE-2017-6931, CVE-2017-6932
Other:
  URL:https://www.drupal.org/sa-core-2018-001
```

Medium (CVSS: 6.8)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
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 Linux

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.808615

Version used: `$Revision: 12051 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

[return to 192.168.57.5]

2.1.12 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary

The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.

Vulnerability Insight

The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: `SSH Weak Encryption Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105611

Version used: `$Revision: 13581 $`

References

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

Medium (CVSS: 4.3)

NVT: OpenSSH Security Bypass Vulnerability

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

This host is running OpenSSH and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     6.9
Installation
path / port:       22/tcp
```

Impact

Successful exploitation will allow remote attackers to bypass intended access restrictions.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Upgrade to OpenSSH version 6.9 or later.

Affected Software/OS
OpenSSH versions before 6.9.

Vulnerability Insight
The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806049
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2015-5352
Other:
  URL:http://openwall.com/lists/oss-security/2015/07/01/10
```

Medium (CVSS: 4.6)
NVT: OpenSSH Client Information Leak

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicious or compromised servers.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.1p2
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        22/tcp
```

Solution

Solution type: VendorFix
Update to 7.1p2 or newer.

Affected Software/OS

OpenSSH >= 5.4 < 7.1p2

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Client Information Leak`
OID:1.3.6.1.4.1.25623.1.0.105512
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-0777, CVE-2016-0778
Other:
  URL:http://www.openssh.com/txt/release-7.1p2
```

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability - Jan16

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.1p2
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.1p2 or later.

Affected Software/OS
OpenSSH versions before 7.1p2.

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806671
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-1907
Other:
  URL:http://www.openssh.com/txt/release-7.1p2
   URL:https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a78
↪9277bb0733ca36e1c0
```

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     None
Installation
path / port:       22/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution

Solution type: NoneAvailable

No known solution is available as of 21th May, 2019. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight

The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method

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

Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.813888

Version used: `2019-05-21T12:48:06+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2018-15919
Other:
  URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

Medium (CVSS: 5.0)

NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.6
Installation
path / port:       22/tcp
```

Impact

Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.6 or later.

Affected Software/OS

OpenSSH versions before 7.6 on Linux

Vulnerability Insight

The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method

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

Details: `OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.812051

Version used: `2019-05-23T14:08:05+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2017-15906
BID:101552
Other:
  URL:https://www.openssh.com/txt/release-7.6
   URL:https://github.com/openbsd/src/commit/a6981567e8e
```

Medium (CVSS: 5.0)

NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.8
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: `2019-05-23T14:08:05+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2018-15473
Other:
  URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Medium (CVSS: 5.5)
NVT: OpenSSH <= 7.2p1 - Xauth Injection

Product detection result

```
cpe:/a:openbsd:openssh:6.6.1p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

openssh xauth command injection may lead to forced-command and /bin/false bypass

Vulnerability Detection Result

```
Installed version: 6.6.1p1
Fixed version:     7.2p2
Installation
path / port:       22/tcp
```

Impact

By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2p2 or later.

Affected Software/OS

OpenSSH versions before 7.2p2.

Vulnerability Insight

An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `OpenSSH <= 7.2p1 - Xauth Injection`
OID:1.3.6.1.4.1.25623.1.0.105581
Version used: `2019-05-22T07:58:25+0000`

Product Detection Result

Product: `cpe:/a:openbsd:openssh:6.6.1p1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-3115
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://www.openssh.com/txt/release-7.2p2
```

[return to 192.168.57.5]

2.1.13 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 115066831
Packet 2: 115067104
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 192.168.57.5]

2.1.14 Low 445/tcp

Low (CVSS: 3.3)
NVT: Samba >= 3.0.25, <= 4.5.2 Multiple Vulnerabilities

Product detection result

```
cpe:/a:samba:samba:4.3.11
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

Samba is prone to a privilege delegation vulnerability.

Vulnerability Detection Result

```
Installed version: 4.3.11
Fixed version:     4.3.13
Installation
path / port:       445/tcp
```

Impact

Successful exploitation would allow an authenticated attacker to gain additional access rights.

Solution

Solution type: VendorFix

Update to version 4.3.13, 4.4.8 or 4.5.3 respectively.

Affected Software/OS

Samba versions 3.0.25 through 4.3.12, 4.4.0 through 4.4.7 and 4.5.0 through 4.5.2.

Vulnerability Insight

Samba always requests forwardable tickets when using Kerberos authentication. A service to which Samba authenticated using Kerberos could subsequently use the ticket to impersonate Samba to other services or domain users.

Vulnerability Detection Method

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

Details: `Samba >= 3.0.25, <= 4.5.2 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.113288

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 13394 $`

Product Detection Result
Product: `cpe:/a:samba:samba:4.3.11`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2016-2125
Other:
  URL:https://www.samba.org/samba/security/CVE-2016-2125.html
```

[return to 192.168.57.5]

2.1.15 Low 21/tcp

Low (CVSS: 2.1)
NVT: ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability

Product detection result

```
cpe:/a:proftpd:proftpd:1.3.5
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)
```

Summary
This host is running ProFTPD server and is prone to local security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.5
Fixed version:     1.3.5e/1.3.6rc5
```

Impact
Successful exploitation will allows attackers to bypass certain security restrictions and perform unauthorized actions.

Solution
Solution type: VendorFix
Upgrade ProFTPD 1.3.5e, 1.3.6rc5 or later.

Affected Software/OS
ProFTPD versions prior to 1.3.5e and 1.3.6 prior to 1.3.6rc5 are vulnerable.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The ProFTPD controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.810731
Version used: `$Revision: 11888 $`

Product Detection Result
Product: `cpe:/a:proftpd:proftpd:1.3.5`
Method: `ProFTPD Server Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.900815)

References

```
CVE: CVE-2017-7418
BID:97409
Other:
  URL:http://bugs.proftpd.org/show_bug.cgi?id=4295
   URL:https://github.com/proftpd/proftpd/commit/ecff21e0d0e84f35c299ef91d7fda08
↪8e516d4ed
   URL:https://github.com/proftpd/proftpd/commit/f59593e6ff730b832dbe8754916cb5c
↪821db579f
   URL:https://github.com/proftpd/proftpd/pull/444/commits/349addc3be4fcdad9bd4e
↪c01ad1ccd916c898ed8
   URL:http://www.proftpd.org
```

[return to 192.168.57.5]

2.1.16 Low 80/tcp

Low (CVSS: 1.9)
NVT: PHP Security Bypass Vulnerability May18 (Linux)

Product detection result

```
cpe:/a:php:php:5.4.5
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: 5.4.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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. Please see the references for more information.

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 Linux.

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813162
Version used: `2019-05-03T08:55:39+0000`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
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
   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: 2.6)
NVT: PHP Information Disclosure Vulnerability - 01 - Sep14

Product detection result

`cpe:/a:php:php:5.4.5`

. . . 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

This host is installed with PHP and is prone to information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.5
Fixed version:     5.3.29/5.4.30/5.5.14
```

Impact

Successful exploitation will allow a local attacker to gain access to sensitive information.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.3.29 or 5.4.30 or 5.5.14 or later.

Affected Software/OS

PHP before version 5.3.x before 5.3.29, 5.4.x before 5.4.30, 5.5.x before 5.5.14

Vulnerability Insight

The flaw is due to an error in the 'hp_print_info' function within /ext/standard/info.c script.

Vulnerability Detection Method

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

Details: `PHP Information Disclosure Vulnerability - 01 - Sep14`

OID:1.3.6.1.4.1.25623.1.0.804849

Version used: `$Revision: 11867 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`

Method: `PHP Version Detection (Remote)`

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-4721
BID:68423
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=67498
   URL:https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html
```

Low (CVSS: 3.3)

NVT: PHP Symlink Attack Vulnerability (Linux)

... continues on next page ...

. . . continued from previous page . . .

Product detection result

```
cpe:/a:php:php:5.4.5
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 symlink attack vulnerability.

Vulnerability Detection Result

```
Installed version: 5.4.5
Fixed version:     5.4.30
```

Impact

Successfully exploiting this issue allows local users to overwrite arbitrary files via a symlink attack on the '/tmp/phpglibccheck' file.

Solution

Solution type: VendorFix

Update to PHP version 5.5.14 or 5.4.30 or 5.3.29 or later.

Affected Software/OS

PHP versions 5.5.x before 5.5.14, 5.4.x before 5.4.30, 5.3.x before 5.3.29 on Linux

Vulnerability Insight

The flaw is due to insecure temporary file use in the configure script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `PHP Symlink Attack Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809736
Version used: `$Revision: 12313 $`

Product Detection Result

Product: `cpe:/a:php:php:5.4.5`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
CVE: CVE-2014-3981
BID:67837
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:https://bugs.php.net/bug.php?id=67390
   URL:http://seclists.org/fulldisclosure/2014/Jun/21
   URL:http://www.php.net
```

Low (CVSS: 3.5)
NVT: Drupal XSS Vulnerability (SA-CORE-2019-004) (Linux)

Product detection result

```
cpe:/a:drupal:drupal:7.5
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

Under certain circumstances the File module/subsystem allows a malicious user to upload a file that can trigger a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 7.5
Fixed version:     7.65
```

Solution

Solution type: VendorFix
Update to version 7.65, 8.5.14, 8.6.13 or later.

Affected Software/OS

Drupal 7, 8.5.x and 8.6.x.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Drupal XSS Vulnerability (SA-CORE-2019-004) (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142159
Version used: `2019-04-23T06:31:54+0000`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7.5`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2019-6341
Other:
  URL:https://www.drupal.org/sa-core-2019-004
```

[return to 192.168.57.5]

2.1.17 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

Solution

Solution type: Mitigation

Disable the weak MAC algorithms.

Vulnerability Detection Method

Details: `SSH Weak MAC Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: `$Revision: 13581 $`

[return to 192.168.57.5]