Scan Report

April 16, 2018

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 "Tests". The scan started at Mon Apr 16 12:04:14 2018 UTC and ended at Mon Apr 16 12:36:43 2018 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
192.168.234.131	12	18	3	0	0
192.168.234.130	4	15	1	0	0
Total: 2	16	33	4	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 53 results selected by the filtering described above. Before filtering there were 377 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.234.131

Host scan start Mon Apr 16 12:05:48 2018 UTC
Host scan end Mon Apr 16 12:36:43 2018 UTC

Service (Port)	Threat Level
8787/tcp	High
5432/tcp	High
general/tcp	High
5900/tcp	High
6200/tcp	High
80/tcp	High
1524/tcp	High
21/tcp	High
5432/tcp	Medium

. . . (continues) . . .

... (continued) ...

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

2.1.1 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se
↪nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m
↪ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution
Solution type: Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:
- Implementing taint on untrusted input

... continues on next page ...

... continued from previous page ...

- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details:`Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `$Revision: 4387 $`

References
`BID:47071`
`Other:`
`URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750`
`URL:http://www.securityfocus.com/bid/47071`
`URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t`
`↪esters/`
`URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html`

[return to 192.168.234.131]

2.1.2 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result
`It was possible to login as user postgres with password "postgres".`

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Details:`PostgreSQL weak password`
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: `$Revision: 8889 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

[return to 192.168.234.131]

2.1.3 High general/tcp

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

Product detection result
cpe:/o:canonical:ubuntu_linux:8.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

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

Vulnerability Detection Result
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP: 8.04
EOL date: 2013-05-09
EOL info: https://wiki.ubuntu.com/Releases

Solution
Solution type: Mitigation

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

Product Detection Result
Product: cpe:/o:canonical:ubuntu_linux:8.04
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.234.131]

2.1.4 High 5900/tcp

High (CVSS: 9.0) NVT: VNC Brute Force Login
Summary Try to log in with given passwords via VNC protocol.
Vulnerability Detection Result `It was possible to connect to the VNC server with the password: password`
Solution **Solution type:** Mitigation Change the password to something hard to guess.
Vulnerability Insight This script tries to authenticate to a VNC server with the passwords set in the password preference. Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.
Vulnerability Detection Method Details:`VNC Brute Force Login` OID:1.3.6.1.4.1.25623.1.0.106056 Version used: `$Revision: 4472 $`

[return to 192.168.234.131]

2.1.5 High 6200/tcp

High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
Summary vsftpd is prone to a backdoor vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
Solution **Solution type:** VendorFix

. . . continues on next page . . .

... continued from previous page ...

The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 5026 $

References
BID:48539
Other:
URL:http://www.securityfocus.com/bid/48539
URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
URL:https://security.appspot.com/vsftpd.html

[return to 192.168.234.131]

2.1.6 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to, - %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details:`TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `$Revision: 4227 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
```
CVE: CVE-2008-5304, CVE-2008-5305
BID:32668, 32669
Other:
  URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
   URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305
```

High (CVSS: 7.5)
NVT: phpinfo() output accessible

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.

Vulnerability Detection Result
```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information to the remote attacker:
http://192.168.234.131/phpinfo.php
http://192.168.234.131/mutillidae/phpinfo.php
```

Impact
Some of the information that can be gathered from this file includes:

... continues on next page ...

... continued from previous page ...

The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:`phpinfo() output accessible`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 6355 $`

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities

Product detection result
`cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
`Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.`
`↪0.901001)`

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability
- An unspecified vulnerability

Vulnerability Detection Result
`Installed version: 1.9.5`
`Fixed version:     4.2`

Impact
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS
Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method
Details:`Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100537

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
URL:http://www.securityfocus.com/bid/38608
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
↪34
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
↪46
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪24
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪35
URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
Vulnerable url: http://192.168.234.131/cgi-bin/php

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer other attacks are also possible.

Solution
Solution type: VendorFix
PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://localhost/index.php?-s

Vulnerability Detection Method
Details:PHP-CGI-based setups vulnerability when parsing query string parameters from ph.
↪..
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: $Revision: 5958 $

References
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
URL:http://www.kb.cert.org/vuls/id/520827
URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
URL:https://bugs.php.net/bug.php?id=61910
URL:http://www.php.net/manual/en/security.cgi-bin.php
URL:http://www.securityfocus.com/bid/53388

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://192.168.234.131/dav/puttest503335255.html
We could delete the following files via the DELETE method at this web server:
http://192.168.234.131/dav/puttest503335255.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

... continues on next page ...

. . . continued from previous page . . .

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: `$Revision: 9335 $`

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

[return to 192.168.234.131]

2.1.7 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host

Vulnerability Detection Result
`The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)`

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution
Solution type: Workaround

Vulnerability Detection Method
Details:`Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `$Revision: 8233 $`

[return to 192.168.234.131]

2.1.8 High 21/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution
Solution type: VendorFix
The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:`vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 5026 $`

References
```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 192.168.234.131]

2.1.9 Medium 5432/tcp

Medium (CVSS: 6.8)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

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

. . . continues on next page . . .

... continued from previous page ...

Impact
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution
Solution type: VendorFix
Updates are available.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h

Vulnerability Insight
OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details:SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: $Revision: 7578 $

References
CVE: CVE-2014-0224
BID:67899
Other:
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6

... continues on next page ...

... continued from previous page ...

```
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details:`SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 7248 $`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8
↪02067) NVT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details:SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: $Revision: 5547 $

References
CVE: CVE-2016-0800, CVE-2014-3566
Other:
URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://drownattack.com/
URL:https://www.imperialviolet.org/2014/10/14/poodle.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:

... continues on next page ...

... continued from previous page ...

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 5525 $

References
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

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

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Impact Level: Application

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details:SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4749 $

References
CVE: CVE-2014-3566
BID:70574
Other:
URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
URL:https://www.imperialviolet.org/2014/10/14/poodle.html
URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm: sha1WithRSAEncryption

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

... continues on next page ...

... continued from previous page ...

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details:`SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 8810 $`

References
```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 1024 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 7578 $

References
Other:
URL:https://weakdh.org/
URL:https://weakdh.org/sysadmin.html

[return to 192.168.234.131]

2.1.10 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

... continues on next page ...

... continued from previous page ...

rijndael-cbc@lysator.liu.se

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: 4490 $

References
Other:
URL:https://tools.ietf.org/html/rfc4253#section-6.3
URL:https://www.kb.cert.org/vuls/id/958563

[return to 192.168.234.131]

2.1.11 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.2

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later, For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details:`TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `$Revision: 4293 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2009-4898`
`Other:`
`URL:http://www.openwall.com/lists/oss-security/2010/08/03/8`
`URL:http://www.openwall.com/lists/oss-security/2010/08/02/17`
`URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix`

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.1

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later, http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details:TWiki Cross-Site Request Forgery Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: $Revision: 4892 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2009-1339
Other:
URL:http://secunia.com/advisories/34880
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
↪ff-cve-2009-1339.txt

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.

... continues on next page ...

... continued from previous page ...

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

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

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

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

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

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

Vulnerability Detection Method
Details:`HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 8888 $`

References
`CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2010-0386`
`BID:9506, 9561, 11604, 15222, 33374, 37995`
`Other:`
`URL:http://www.kb.cert.org/vuls/id/288308`
`URL:http://www.kb.cert.org/vuls/id/867593`
`URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable`
`URL:https://www.owasp.org/index.php/Cross_Site_Tracing`

Medium (CVSS: 5.0)
NVT: /doc directory browsable

Summary
The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection Result
`Vulnerable url: http://192.168.234.131/doc/`

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
<Directory /usr/doc> AllowOverride None order deny,allow deny from all allow from localhost </Directory>

Vulnerability Detection Method
Details:`/doc directory browsable`
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: `$Revision: 4288 $`

References
`CVE: CVE-1999-0678`
`BID:318`

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Product detection result
`cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
`Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.`
`↪0.901001)`

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result
`Installed version: 1.9.5`
`Fixed version: 12.11`

Impact
Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later. For updates refer to https://tiki.org

Affected Software/OS
Tiki Wiki CMS Groupware versions:
- below 12.11 LTS

... continues on next page ...

... continued from previous page ...

- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight
The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check the version is vulnerable or not.
Details:`Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: `$Revision: 5144 $`

Product Detection Result
Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
```
CVE: CVE-2016-10143
Other:
  URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-
↪released
   URL:https://sourceforge.net/p/tikiwiki/code/60308/
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability

Product detection result
```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result
```
Installed version: 1.9.5
Fixed version:     2.2
```

Impact
Successful exploitation could allow arbitrary code execution in the context of an affected site.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki&bl

Affected Software/OS
Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight
The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method
Details:`Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: `$Revision: 5144 $`

Product Detection Result
Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
`CVE: CVE-2008-5318, CVE-2008-5319`
`Other:`
`URL:http://secunia.com/advisories/32341`
`URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41`

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary
awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
`Vulnerable url: http://192.168.234.131/mutillidae/index.php?page=/etc/passwd`

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host other attacks are also possible.

Solution
Solution type: WillNotFix

... continues on next page ...

... continued from previous page ...

No solution or patch was made available for at least one year since 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
awiki 20100125 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`awiki Multiple Local File Include Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: `$Revision: 7577 $`

References
`BID:49187`
`Other:`
`URL:http://www.securityfocus.com/bid/49187`
`URL:http://www.kobaonline.com/awiki/`

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 6720 $

References
CVE: CVE-2012-0053
BID:51706
Other:
URL:http://secunia.com/advisories/47779
URL:http://www.exploit-db.com/exploits/18442
URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
URL:http://httpd.apache.org/security/vulnerabilities_22.html
URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

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

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since 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
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: $Revision: 5323 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4480
Other:
URL:http://www.exploit-db.com/exploits/15699/
URL:http://www.vupen.com/english/advisories/2010/3133

[return to 192.168.234.131]

2.1.12 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Check for Anonymous FTP Login

Summary
This FTP Server allows anonymous logins.

Vulnerability Detection Result
It was possible to login to the remote FTP service with the following anonymous account:
anonymous:openvas@example.com
ftp:openvas@example.com

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files

Solution
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Try to login with an anonymous account at the remove FTP service.
Details:`Check for Anonymous FTP Login`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `$Revision: 8146 $`

References
`Other:`
`URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497`

[return to 192.168.234.131]

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: 59701
Packet 2: 59807
```

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.

... continues on next page ...

... continued from previous page ...

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: 9035 $`

References
```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.234.131]

2.1.14 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

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-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: $Revision: 4490 $

[return to 192.168.234.131]

2.1.15 Low 80/tcp

Low (CVSS: 3.5)
NVT: Tiki Wiki CMS Groupware XSS Vulnerability

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
An XSS vulnerability (via an SVG image) in Tiki allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/filegals/filegallib.php.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 18.0

Solution
Solution type: VendorFix
Upgrade to version 18.0 or later.

Affected Software/OS
Tiki Wiki CMS Groupware prior to version 18.0.

Vulnerability Detection Method
Checks the version.
Details:Tiki Wiki CMS Groupware XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.140797
Version used: $Revision: 9171 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References

... continues on next page ...

... continued from previous page ...

```
CVE: CVE-2018-7188
Other:
  URL:http://openwall.com/lists/oss-security/2018/02/16/1
```

[return to 192.168.234.131]

2.2 192.168.234.130

Host scan start Mon Apr 16 12:05:47 2018 UTC
Host scan end Mon Apr 16 12:17:39 2018 UTC

Service (Port)	Threat Level
80/tcp	High
443/tcp	High
135/tcp	Medium
80/tcp	Medium
443/tcp	Medium
general/tcp	Low

2.2.1 High 80/tcp

High (CVSS: 7.5)
NVT: phpinfo() output accessible

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information to the remote attacker:
http://192.168.234.130/dashboard/phpinfo.php
```

Impact
Some of the information that can be gathered from this file includes:
The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:phpinfo() output accessible
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: $Revision: 6355 $

High (CVSS: 7.5)
NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)

Product detection result
cpe:/a:php:php:7.2.1
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: 7.2.1
Fixed version: 7.2.3
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.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later. For updates refer to http://www.php.net.

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

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812820
Version used: $Revision: 9299 $

... continues on next page ...

. . . continued from previous page . . .

Product Detection Result
Product: cpe:/a:php:php:7.2.1
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

[return to 192.168.234.130]

2.2.2 High 443/tcp

High (CVSS: 7.5)
NVT: phpinfo() output accessible

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.

Vulnerability Detection Result
The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker:
https://192.168.234.130/dashboard/phpinfo.php

Impact
Some of the information that can be gathered from this file includes:
The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:phpinfo() output accessible
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: $Revision: 6355 $

High (CVSS: 7.5)
NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)

Product detection result
`cpe:/a:php:php:7.2.1`
`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: 7.2.1`
`Fixed version: 7.2.3`
`Installation path / port: 443/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.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later. For updates refer to http://www.php.net.

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

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812820
Version used: `$Revision: 9299 $`

Product Detection Result
Product: `cpe:/a:php:php:7.2.1`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

. . . continues on next page . . .

... continued from previous page ...

References

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

[return to 192.168.234.130]

2.2.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 1025/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1025]
Port: 1026/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1026]
     Annotation: Security Center
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1026]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1026]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1026]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1026]
     Annotation: Event log TCPIP
Port: 1027/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1027]
     Named pipe : lsass
```

... continues on next page ...

... continued from previous page ...

```
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 1028/tcp
     UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: AppInfo
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: IP Transition Configuration endpoint
     UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: AppInfo
     UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: AppInfo
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: IKE/Authip API
     UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1028]
     Annotation: AppInfo
Port: 1029/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.234.130[1029]
Port: 1030/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1030]
     Annotation: IPSec Policy agent endpoint
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.234.130[1030]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details:DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

[return to 192.168.234.130]

2.2.4 Medium 80/tcp

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

Product detection result
cpe:/a:php:php:7.2.1
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: 7.2.1
Fixed version: NoneAvailable
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.
Impact Level: Application

Solution
Solution type: NoneAvailable
No solution or patch is available as of 20th Feb, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x to 5.4.43 and 7.x to 7.2.2 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
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.812519
Version used: $Revision: 9180 $

Product Detection Result
Product: cpe:/a:php:php:7.2.1
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=70185
URL:https://bugs.php.net/bug.php?id=75968
URL:https://www.futureweb.at/security/CVE-2015-9253
URL:https://vuldb.com//?id.113566

Medium (CVSS: 5.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)

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

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.30
Installation
path / port: 80/tcp

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

Solution

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812846
Version used: `$Revision: 9404 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Version 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: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

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

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

... continues on next page ...

... continued from previous page ...

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

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

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

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

Vulnerability Detection Method
Details:`HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 8888 $`

References
```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2010-0386
BID:9506, 9561, 11604, 15222, 33374, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 5.4)
NVT: Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)

Product detection result
```
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)
```

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

Vulnerability Detection Result
```
Installed version: 2.4.29
Fixed version:     2.4.30
```

... continues on next page ...

... continued from previous page ...

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

Impact
Successful exploitation will allow an attacker to destroy an HTTP/2 stream, resulting in a denial of service condition.
Impact Level: Application

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

Affected Software/OS
Apache HTTP server versions 2.4.17, 2.4.18, 2.4.20, 2.4.23 and from 2.4.25 to 2.4.29 on Windows.

Vulnerability Insight
The flaw exists as the Apache HTTP Server writes a NULL pointer potentially to an already freed memory.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812850
Version used: `$Revision: 9404 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
```
CVE: CVE-2018-1302
BID:103528
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:http://www.openwall.com/lists/oss-security/2018/03/24/8
   URL:http://www.openwall.com/lists/oss-security/2018/03/24/2
```

Medium (CVSS: 5.4)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004`
`↪98)`

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result
```
Installed version: 2.4.29
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.
Impact Level: Application

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

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

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812847
Version used: `$Revision: 9404 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

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

[return to 192.168.234.130]

2.2.5 Medium 443/tcp

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

Product detection result
`cpe:/a:php:php:7.2.1`
`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: 7.2.1`
`Fixed version: NoneAvailable`
`Installation path / port: 443/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.
Impact Level: Application

Solution
Solution type: NoneAvailable
No solution or patch is available as of 20th Feb, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x to 5.4.43 and 7.x to 7.2.2 on Windows.

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812519
Version used: `$Revision: 9180 $`

Product Detection Result

. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:php:php:7.2.1
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=70185
URL:https://bugs.php.net/bug.php?id=75968
URL:https://www.futureweb.at/security/CVE-2015-9253
URL:https://vuldb.com//?id.113566

Medium (CVSS: 5.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Version 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: 2.4.29
Fixed version: 2.4.30
Installation
path / port: 443/tcp

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

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

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

Vulnerability Insight
Multiple flaws exists due to,

... continues on next page ...

... continued from previous page ...

- 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
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812846
Version used: `$Revision: 9404 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Version 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: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

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

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

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

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Web servers with enabled TRACE and/or TRACK methods.

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

Vulnerability Detection Method
Details:`HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 8888 $`

References
`CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2010-0386`
`BID:9506, 9561, 11604, 15222, 33374, 37995`
`Other:`
`URL:http://www.kb.cert.org/vuls/id/288308`
`URL:http://www.kb.cert.org/vuls/id/867593`
`URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable`
`URL:https://www.owasp.org/index.php/Cross_Site_Tracing`

Medium (CVSS: 5.4)
NVT: Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004`
`↪98)`

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

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.30`
`Installation`
`path / port: 443/tcp`

Impact
Successful exploitation will allow an attacker to destroy an HTTP/2 stream, resulting in a denial of service condition.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
Apache HTTP server versions 2.4.17, 2.4.18, 2.4.20, 2.4.23 and from 2.4.25 to 2.4.29 on Windows.

Vulnerability Insight
The flaw exists as the Apache HTTP Server writes a NULL pointer potentially to an already freed memory.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812850
Version used: `$Revision: 9404 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
```
CVE: CVE-2018-1302
BID:103528
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:http://www.openwall.com/lists/oss-security/2018/03/24/8
   URL:http://www.openwall.com/lists/oss-security/2018/03/24/2
```

Medium (CVSS: 5.4)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)

Product detection result
```
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)
```

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

Vulnerability Detection Result
```
Installed version: 2.4.29
Fixed version:     2.4.30
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 443/tcp

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

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

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

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

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812847
Version used: $Revision: 9404 $

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: Untrusted Certificate Authorities

Summary
The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted Certi
↪ficate Authority:
Issuer: CN=localhost
Certificate details:
subject ...: CN=localhost
subject alternative names (SAN):
None
issued by .: CN=localhost
serial ....: 00B5C752C98781B503
valid from : 2009-11-10 23:48:47 UTC
valid until: 2019-11-08 23:48:47 UTC
fingerprint (SHA-1): B0238C547A905BFA119C4E8BACCAEACF36491FF6
fingerprint (SHA-256): 016973380C0F1DF00BD9593ED8D5EFA3706CD6DF7993F6141272B8052
↪2ACDD23
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted certificate authority.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority.
Details:`SSL/TLS: Untrusted Certificate Authorities`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `$Revision: 8740 $`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Solution
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 5525 $

References
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure signature algorithms:
Subject: CN=localhost
Signature Algorithm: sha1WithRSAEncryption

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details:`SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 8810 $`

References
```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 7578 $

References
Other:
URL:https://weakdh.org/
URL:https://weakdh.org/sysadmin.html

[return to 192.168.234.130]

2.2.6 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: 565104
Packet 2: 565214

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

... continues on next page ...

... continued from previous page ...

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: 9035 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

[return to 192.168.234.130]