Scan Report

July 20, 2023

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 "RACE-HIST". The scan started at Thu Jul 20 00:00:14 2023 UTC and ended at Thu Jul 20 01:30:01 2023 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
10.0.0.21 ip-10-0-0-21.us-east-2.compute.internal	167	202	18	0	0
Total: 1	167	202	18	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is excluded from the report.
Notes are excluded from the report.
This report might not show details of all issues that were found.
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 387 results selected by the filtering described above. Before filtering there were 629 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.21 - ip-10-0-0-21.us-east-2.compute.internal	SSH	Success	Protocol SSH, Port 22, User vagrant

2 Results per Host

2.1 10.0.0.21

Host scan start	Thu Jul 20 00:01:00 2023 UTC
Host scan end	Thu Jul 20 01:29:51 2023 UTC

Service (Port)	Threat Level
21/tcp	High
8383/tcp	High
general/tcp	High
8484/tcp	High
22/tcp	High
8585/tcp	High
8020/tcp	High
1617/tcp	High
9200/tcp	High

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
445/tcp	High
3306/tcp	High
4848/tcp	High
80/tcp	High
21/tcp	Medium
8383/tcp	Medium
8484/tcp	Medium
22/tcp	Medium
8181/tcp	Medium
135/tcp	Medium
8585/tcp	Medium
3920/tcp	Medium
8020/tcp	Medium
3389/tcp	Medium
9200/tcp	Medium
3306/tcp	Medium
49234/tcp	Medium
4848/tcp	Medium
general/tcp	Low
general/icmp	Low
8585/tcp	Low
9200/tcp	Low
3306/tcp	Low
49234/tcp	Low

2.1.1 High 21/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`vagrant:vagrant`

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-07-06T05:05:36Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2001-1594`
`cve: CVE-2013-7404`
`cve: CVE-2018-19063`
`cve: CVE-2018-19064`

[return to 10.0.0.21]

2.1.2 High 8383/tcp

High (CVSS: 7.5)
NVT: '/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Vulnerable URL: https://ip-10-0-0-21.us-east-2.compute.internal:8383/.//WEB-INF/
↪web.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
```

... continues on next page ...

... continued from previous page ...

```
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and/or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

The following vendor fixes are known:
- Update to Payara Platform Enterprise 5.31.0, Payara Platform Community 5.2021.7 or later.
For other products please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Payara Platform Enterprise / Community
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/.//WEB-INF/web.xml
http://example.com/.//web-inf/web.xml
(note the './/' before 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: `2023-03-06T10:19:58Z`

References
`cve: CVE-2021-41381`
`url: https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-`
`↪054.txt`
`url: http://packetstormsecurity.com/files/164365/Payara-Micro-Community-5.2021.6`
`↪-Directory-Traversal.html`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
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_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)`
`TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)`
`TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)`

... continues on next page ...

... continued from previous page ...

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
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: 2022-08-01T10:11:45Z

References
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[return to 10.0.0.21]

2.1.3 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)
used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result
```
Version of installed component:          22.7.2 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10
↪)
Latest available openvas-scanner version: 22.7.3
Reference URL(s) for the latest available version: https://forum.greenbone.net/t
↪/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
```

Solution:
Solution type: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method
Details: `Report outdated / end-of-life Scan Engine / Environment (local)`
OID:1.3.6.1.4.1.25623.1.0.108560
Version used: `2023-07-19T05:05:15Z`

References
```
url: https://www.greenbone.net/en/testnow/
url: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initi
↪al-release-2022-07-25/12638
url: https://forum.greenbone.net/t/greenbone-community-edition-21-04-end-of-life
↪/13837
url: https://forum.greenbone.net/t/gvm-21-04-end-of-life-initial-release-2021-04
↪-16/8942
```

... continues on next page ...

... continued from previous page ...

url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08
↪-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14
↪/3674
url: https://forum.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-04-05
↪/208
url: https://forum.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03-07/
↪211
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#creating-an
↪-override

[return to 10.0.0.21]

2.1.4 High 8484/tcp

High (CVSS: 10.0)
NVT: Jenkins CI Groovy Console accessible

Summary
Checks if the Jenkins CI Groovy Console is unprotected.

Vulnerability Detection Result
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8484/script

Impact
The Groovy Console allows an attacker to execute operating system commands with the permissions of the user running the service.

Solution:
Solution type: Mitigation
Protect the access to the Groovy Console by configuring user accounts. Please see the reference for more information.

Vulnerability Detection Method
The script sends a HTTP request to the server and checks if the Groovy Console is unprotected.
Details: Jenkins CI Groovy Console accessible
OID:1.3.6.1.4.1.25623.1.0.111002
Version used: 2020-05-08T08:34:44Z

References
url: https://wiki.jenkins-ci.org/display/JENKINS/Securing+Jenkins

High (CVSS: 9.8)
NVT: Jenkins Multiple Vulnerabilities (Feb 2016) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 1.650`
`Installation path / port: /`

Impact
Successful exploitation will allow remote attackers to obtain sensitive information, bypass the protection mechanism, gain elevated privileges, bypass intended access restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Jenkins main line users should update to 1.650, Jenkins LTS users should update to 1.642.2.

Affected Software/OS
Jenkins main line 1.649 and prior, Jenkins LTS 1.642.1 and prior.

Vulnerability Insight
Multiple flaws are due to:
- The verification of user-provided API tokens with the expected value did not use a constant-time comparison algorithm, potentially allowing attackers to use statistical methods to determine valid API tokens using brute-force methods.
- The verification of user-provided CSRF crumbs with the expected value did not use a constant-time comparison algorithm, potentially allowing attackers to use statistical methods to determine valid CSRF crumbs using brute-force methods.
- The Jenkins has several API endpoints that allow low-privilege users to POST XML files that then get deserialized by Jenkins. Maliciously crafted XML files sent to these API endpoints could result in arbitrary code execution.
- An HTTP response splitting vulnerability in the CLI command documentation allowed attackers to craft Jenkins URLs that serve malicious content.
- The Jenkins remoting module allowed unauthenticated remote attackers to open a JRMP listener on the server hosting the Jenkins master process, which allowed arbitrary code execution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins Multiple Vulnerabilities (Feb 2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.807331
Version used: `2021-10-08T08:23:39Z`

References
. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2016-0788
cve: CVE-2016-0789
cve: CVE-2016-0790
cve: CVE-2016-0791
cve: CVE-2016-0792
url: https://jenkins.io/security/advisory/2016-02-24/
url: https://www.contrastsecurity.com/security-influencers/serialization-must-di
↪e-act-2-xstream
cert-bund: CB-K16/1303
cert-bund: CB-K16/0311
dfn-cert: DFN-CERT-2016-1386
dfn-cert: DFN-CERT-2016-0338
```

High (CVSS: 9.8)
NVT: Jenkins Multiple Vulnerabilities (Apr 2017) - Windows

Summary
Multiple Cross-Site Request Forgery vulnerabilities in Jenkins allow malicious users to perform several administrative actions by tricking a victim into opening a web page.

Vulnerability Detection Result

```
Installed version: 1.637
Fixed version:     2.57
Installation
path / port:       /
```

Impact
Successfully exploiting this issue allows attackers to:
- perform several administrative actions by tricking a victim into opening a web page.execute arbitrary code in the context of the affected application.
- to transfer a serialized Java SignedObject object to the remoting-based Jenkins CLI, that would be deserialized using a new ObjectInputStream, bypassing the existing blacklist-based protection mechanism.
- impersonate any other Jenkins user on the same instance.
- crash the Java process.

Solution:
Solution type: VendorFix
Jenkins main line users should update to 2.57, Jenkins LTS users should update to 2.46.2.

Affected Software/OS
Jenkins main line 2.56 and prior, Jenkins LTS 2.46.1 and prior.

Vulnerability Insight
Multiple flaws are due to:
- multiple Cross-Site Request Forgery vulnerabilities.

... continues on next page ...

... continued from previous page ...

- the storage of the encrypted user name in a cache file which is used to authenticate further commands.
- XStream library which allow anyone able to provide XML to Jenkins for processing using XStream to crash the Java process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins Multiple Vulnerabilities (Apr 2017) - Windows`
OID:1.3.6.1.4.1.25623.1.0.107157
Version used: `2022-06-15T03:04:08Z`

References
`cve: CVE-2017-1000353`
`cve: CVE-2017-1000354`
`cve: CVE-2017-1000355`
`cve: CVE-2017-1000356`
`url: http://www.securityfocus.com/bid/98056`
`url: https://jenkins.io/security/advisory/2017-04-26/`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: CB-K17/0706`
`dfn-cert: DFN-CERT-2017-0727`

High (CVSS: 9.8)
NVT: Jenkins 'Java Deserialization' Remote Code Execution Vulnerability - Windows

Summary
Jenkins is prone to a remote code execution vulnerability.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.32
Installation
path / port:       /
```

Impact
Successfully exploiting this issue allows attackers to execute arbitrary code in the context of the affected application. Failed exploits will result in denial-of-service conditions.

Solution:
Solution type: VendorFix
Upgrade to Jenkins to 2.32 or later / Jenkins LTS to 2.19.3 or later.

Affected Software/OS
Jenkins LTS 2.19.2 and prior, Jenkins 2.31 and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to an Jenkins allowing to transfer a serialized Java object to the Jenkins CLI, making Jenkins connect to an attacker-controlled LDAP server, which in turn can send a serialized payload leading to code execution, bypassing existing protection mechanisms.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins 'Java Deserialization' Remote Code Execution Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.108062
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2016-9299`
`url: https://jenkins.io/security/advisory/2016-11-16/`
`url: http://www.securityfocus.com/bid/94281`
`cert-bund: CB-K16/1809`
`dfn-cert: DFN-CERT-2016-1915`

High (CVSS: 9.8)
NVT: Jenkins < 2.154 and < 2.138.4 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.154`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.154 or later / Jenkins LTS to either 2.138.4 or 2.150.1 or later.

Affected Software/OS
Jenkins LTS up to and including 2.138.3, Jenkins weekly up to and including 2.153.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Code execution through crafted URLs (CVE-2018-1000861).
- Forced migration of user records (CVE-2018-1000863).
- Workspace browser allowed accessing files outside the workspace (CVE-2018-1000862).
- Potential denial of service through cron expression form validation (CVE-2018-1000864).

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.154 and < 2.138.4 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.108512
Version used: 2022-08-09T10:11:17Z

References
cve: CVE-2018-1000861
cve: CVE-2018-1000862
cve: CVE-2018-1000863
cve: CVE-2018-1000864
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://jenkins.io/security/advisory/2018-12-05/
dfn-cert: DFN-CERT-2018-2487

High (CVSS: 9.8)
NVT: Jenkins < 2.303.3, < 2.319 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.319
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 2.319, 2.303.3 LTS or later.

Affected Software/OS
Jenkins version 2.318 and prior and 2.303.2 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-21685, CVE-2021-21686, CVE-2021-21687, CVE-2021-21688, CVE-2021-21689, CVE-2021-21690, CVE-2021-21691, CVE-2021-21692, CVE-2021-21693, CVE-2021-21694, CVE-2021-21695: Bypassing path filtering of agent-to-controller access control
- CVE-2021-21696: Agent-to-controller access control allowed writing to sensitive directory used by Pipeline: Shared Groovy Libraries Plugin
- CVE-2021-21697: Agent-to-controller access control allows reading/writing most content of build directories

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

... continues on next page ...

... continued from previous page ...

Details: Jenkins < 2.303.3, < 2.319 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.147112
Version used: 2021-11-10T03:03:45Z

References
cve: CVE-2021-21685
cve: CVE-2021-21686
cve: CVE-2021-21687
cve: CVE-2021-21688
cve: CVE-2021-21689
cve: CVE-2021-21690
cve: CVE-2021-21691
cve: CVE-2021-21692
cve: CVE-2021-21693
cve: CVE-2021-21694
cve: CVE-2021-21695
cve: CVE-2021-21696
cve: CVE-2021-21697
url: https://www.jenkins.io/security/advisory/2021-11-04/
dfn-cert: DFN-CERT-2021-2487
dfn-cert: DFN-CERT-2021-2308

High (CVSS: 9.4)
NVT: Jenkins < 2.243, < 2.235.5 LTS Buffer Corruption in bundled Jetty - Windows

Summary
Jenkins is prone to a buffer corruption in bundled Jetty.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.243
Installation
path / port: /

Impact
This vulnerability may allow unauthenticated attackers to obtain HTTP response headers that may include sensitive data intended for another user.

Solution:
Solution type: VendorFix
Update to version 2.243, 2.235.5 LTS or later.

Affected Software/OS
Jenkins version 2.242 and prior and 2.235.4 LTS and prior.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

In Eclipse Jetty in case of too large response headers, Jetty throws an exception to produce an HTTP 431 error. When this happens, the ByteBuffer containing the HTTP response headers is released back to the ByteBufferPool twice. Because of this double release, two threads can acquire the same ByteBuffer from the pool and while thread1 is about to use the ByteBuffer to write response1 data, thread2 fills the ByteBuffer with response2 data. Thread1 then proceeds to write the buffer that now contains response2 data.
This results in client1, which issued request1 and expects responses, to see response2 which could contain sensitive data belonging to client2 (HTTP session ids, authentication credentials, etc.).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.243, < 2.235.5 LTS Buffer Corruption in bundled Jetty - Windows`
OID:1.3.6.1.4.1.25623.1.0.112812
Version used: `2021-07-08T11:00:45Z`

References
`cve: CVE-2019-17638`
`url: https://www.jenkins.io/security/advisory/2020-08-17/`
`cert-bund: CB-K20/1023`
`dfn-cert: DFN-CERT-2021-0819`
`dfn-cert: DFN-CERT-2020-2762`
`dfn-cert: DFN-CERT-2020-2141`
`dfn-cert: DFN-CERT-2020-1837`
`dfn-cert: DFN-CERT-2020-1814`

High (CVSS: 9.0)
NVT: Jenkins CSRF Vulnerability (CVE-2023-35141) - Windows

Summary
Jenkins is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.400`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Update to version 2.401.1 (LTS), 2.400 or later.

Affected Software/OS
Jenkins version through 2.387.3 (LTS) and version through 2.399.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

POST requests are sent in order to load the list of context actions. If part of the URL includes insufficiently escaped user-provided values, a victim may be tricked into sending a POST request to an unexpected endpoint by opening a context menu.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins CSRF Vulnerability (CVE-2023-35141) - Windows`
OID:1.3.6.1.4.1.25623.1.0.124338
Version used: `2023-06-20T05:05:27Z`

References
`cve: CVE-2023-35141`
`url: https://www.jenkins.io/security/advisory/2023-06-14/#SECURITY-3135`
`cert-bund: WID-SEC-2023-1471`
`dfn-cert: DFN-CERT-2023-1382`

High (CVSS: 8.8)
NVT: Jenkins Multiple Vulnerabilities (Oct 2017) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.84
Installation
path / port:       /
```

Impact
Successful exploitation will allow remote attackers to obtain sensitive information, and execute arbitrary code.

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.84 or later / Jenkins LTS to 2.73.2 or later.

Affected Software/OS
Jenkins LTS 2.73.1 and prior, Jenkins weekly up to and including 2.83.

Vulnerability Insight
Multiple flaws are due to:
- arbitrary shell command execution
- bundling vulnerable libraries
- disclosing various information
- sending form validation for passwords via GET

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins Multiple Vulnerabilities (Oct 2017) - Windows
OID:1.3.6.1.4.1.25623.1.0.112107
Version used: 2021-10-12T09:28:32Z

References
cve: CVE-2017-1000393
cve: CVE-2017-1000394
cve: CVE-2017-1000395
cve: CVE-2017-1000396
cve: CVE-2017-1000398
cve: CVE-2017-1000399
cve: CVE-2017-1000400
cve: CVE-2017-1000401
cve: CVE-2012-6153
url: https://jenkins.io/security/advisory/2017-10-11/
cert-bund: CB-K15/1508
cert-bund: CB-K15/1506
cert-bund: CB-K15/0678
cert-bund: CB-K15/0391
cert-bund: CB-K15/0330
cert-bund: CB-K15/0186
cert-bund: CB-K15/0148
cert-bund: CB-K14/1598
cert-bund: CB-K14/1485
cert-bund: CB-K14/1035
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2020-2259
dfn-cert: DFN-CERT-2015-1595
dfn-cert: DFN-CERT-2015-1576
dfn-cert: DFN-CERT-2015-0712
dfn-cert: DFN-CERT-2015-0403
dfn-cert: DFN-CERT-2015-0342
dfn-cert: DFN-CERT-2015-0191
dfn-cert: DFN-CERT-2015-0152
dfn-cert: DFN-CERT-2014-1693
dfn-cert: DFN-CERT-2014-1572
dfn-cert: DFN-CERT-2014-1078

High (CVSS: 8.8)
NVT: Jenkins < 2.228, < 2.204.6 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.228
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 2.228, 2.204.6 LTS or later.

Affected Software/OS
Jenkins version 2.227 and prior and 2.204.5 LTS and prior.

Vulnerability Insight
Jenkins is prone to multiple vulnerabilities:
- CSRF protection for any URL could be bypassed (CVE-2020-2160)
- Stored XSS vulnerability in label expression validation (CVE-2020-2161)
- Stored XSS vulnerability in file parameters (CVE-2020-2162)
- Stored XSS vulnerability in list view column headers (CVE-2020-2163)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.228, < 2.204.6 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.143642
Version used: 2021-07-08T11:00:45Z

References
cve: CVE-2020-2160
cve: CVE-2020-2161
cve: CVE-2020-2162
cve: CVE-2020-2163
url: https://jenkins.io/security/advisory/2020-03-25/
dfn-cert: DFN-CERT-2020-1441
dfn-cert: DFN-CERT-2020-0624

High (CVSS: 8.8)
NVT: Jenkins < 2.192 and < 2.176.3 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.192
Installation

... continues on next page ...

... continued from previous page ...

path / port: /

Solution:
Solution type: VendorFix
Update to version 2.176.3 LTS, 2.192 weekly or later.

Affected Software/OS
Jenkins weekly up to and including 2.191 and Jenkins LTS up to and including 2.176.2

Vulnerability Insight
Jenkins is prone to multiple vulnerabilities:
- Stored XSS vulnerability in update center (CVE-2019-10383)
- CSRF protection tokens for anonymous users does not expire in some circumstances (CVE-2019-10384)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.192 and < 2.176.3 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.142824
Version used: 2022-06-15T03:04:08Z

References
cve: CVE-2019-10383
cve: CVE-2019-10384
url: https://jenkins.io/security/advisory/2019-08-28/
dfn-cert: DFN-CERT-2019-1972
dfn-cert: DFN-CERT-2019-1802

High (CVSS: 8.8)
NVT: Jenkins Multiple Vulnerabilities (Feb 2017) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.44
Installation
path / port: /

Impact
Successful exploitation will allow remote attackers to obtain sensitive information, to bypass intended access restrictions and execute arbitrary code.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Jenkins main line to 2.44 or later / Jenkins LTS to 2.32.2 or later.

Affected Software/OS
Jenkins LTS 2.32.1 and prior, Jenkins main line 2.43 and prior.

Vulnerability Insight
Multiple flaws are due to:
- cross-site scripting vulnerabilities
- the usage ouf outdated libraries
- insufficient access permission verifications / checks
- a remote code execution vulnerability
- an information disclosure vulnerability

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins Multiple Vulnerabilities (Feb 2017) - Windows`
OID:1.3.6.1.4.1.25623.1.0.108096
Version used: `2021-10-12T09:28:32Z`

References
`cve: CVE-2011-4969`
`cve: CVE-2015-0886`
`cve: CVE-2017-2598`
`cve: CVE-2017-2599`
`cve: CVE-2017-2600`
`cve: CVE-2017-2601`
`cve: CVE-2017-2602`
`cve: CVE-2017-2603`
`cve: CVE-2017-2604`
`cve: CVE-2017-2605`
`cve: CVE-2017-2606`
`cve: CVE-2017-2607`
`cve: CVE-2017-2608`
`cve: CVE-2017-2609`
`cve: CVE-2017-2610`
`cve: CVE-2017-2611`
`cve: CVE-2017-2612`
`cve: CVE-2017-2613`
`cve: CVE-2017-1000362`
`url: https://jenkins.io/security/advisory/2017-02-01/`
`cert-bund: WID-SEC-2023-0090`
`cert-bund: WID-SEC-2022-1804`
`cert-bund: WID-SEC-2022-0529`
`cert-bund: WID-SEC-2022-0445`
`cert-bund: WID-SEC-2022-0265`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0195
cert-bund: CB-K15/0272
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
dfn-cert: DFN-CERT-2015-0283

High (CVSS: 8.6)
NVT: Jenkins < 2.214, < 2.204.2 LTS Authentication Bypass Vulnerability - Windows

Summary
Jenkins is prone to an inbound TCP Agent Protocol/3 authentication bypass vulnerability.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.214
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 2.214, 2.204.2 LTS or later.

Affected Software/OS
Jenkins version 2.213 and prior and 2.204.1 LTS and prior.

Vulnerability Insight
Jenkins includes support for the Inbound TCP Agent Protocol/3 for communication between master and agents. While this protocol has been deprecated in 2018 and was recently removed from Jenkins in 2.214, it could still easily be enabled in Jenkins LTS 2.204.1, 2.213, and older. This protocol incorrectly reuses encryption parameters which allow an unauthenticated remote attacker to determine the connection secret. This secret can then be used to connect attacker-controlled Jenkins agents to the Jenkins master.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.214, < 2.204.2 LTS Authentication Bypass Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.143438
Version used: 2021-07-08T11:00:45Z

References
cve: CVE-2020-2099
url: https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1682
dfn-cert: DFN-CERT-2020-0207

High (CVSS: 8.5)
NVT: Jenkins < 2.375.4 (LTS), < 2.394 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.394`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Update to version 2.375.4 (LTS), 2.394 or later.

Affected Software/OS
Jenkins version 2.375.3 (LTS) and prior and 2.393 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2023-27899: Temporary plugin file created with insecure permissions
- CVE-2023-24998, CVE-2023-27900, CVE-2023-27901: DoS vulnerability in bundled Apache Commons FileUpload library
- CVE-2023-27902: Workspace temporary directories accessible through directory browser
- CVE-2023-27903: Temporary file parameter created with insecure permissions
- CVE-2023-27904: Information disclosure through error stack traces related to agents

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.375.4 (LTS), < 2.394 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.170357
Version used: `2023-03-10T10:20:36Z`

References
`cve: CVE-2023-27899`
`cve: CVE-2023-24998`
`cve: CVE-2023-27900`
`cve: CVE-2023-27901`
`cve: CVE-2023-27902`
`cve: CVE-2023-27903`
`cve: CVE-2023-27904`
`url: https://www.jenkins.io/security/advisory/2023-03-08/`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1142`
`cert-bund: WID-SEC-2023-1021`
`cert-bund: WID-SEC-2023-1017`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-1012
cert-bund: WID-SEC-2023-1007
cert-bund: WID-SEC-2023-1005
cert-bund: WID-SEC-2023-0609
cert-bund: WID-SEC-2023-0433
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1362
dfn-cert: DFN-CERT-2023-1109
dfn-cert: DFN-CERT-2023-0902
dfn-cert: DFN-CERT-2023-0886
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0830
dfn-cert: DFN-CERT-2023-0763
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2023-0540
dfn-cert: DFN-CERT-2023-0414
```

High (CVSS: 8.1)
NVT: Jenkins CSRF Protection Delay Vulnerability - Windows

Summary
A race condition during Jenkins startup could result in the wrong order of execution of commands during initialization.

Vulnerability Detection Result

```
Installed version: 1.637
Fixed version:     2.95
Installation
path / port:       /
```

Impact
Successfully exploiting this issue would reduce the system security severely.

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.95 or later / Jenkins LTS to 2.89.2 or later.

Affected Software/OS
Jenkins LTS 2.89.1, Jenkins weekly up to and including 2.94.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

There's a very short window of time after startup during which Jenkins may no longer show the 'Please wait while Jenkins is getting ready to work' message, but Cross-Site Request Forgery (CSRF) protection may not yet be effective.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins CSRF Protection Delay Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.112197
Version used: `2021-06-29T11:00:37Z`

References
`cve: CVE-2017-1000504`
`url: https://jenkins.io/security/advisory/2017-12-14/`

High (CVSS: 8.1)
NVT: Jenkins < 2.164.2 LTS and < 2.172 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.172
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 2.164.2 (LTS) and 2.172 (weekly).

Affected Software/OS
Jenkins LTS 2.164.1 and prior and Jenkins weekly 2.171 and prior.

Vulnerability Insight
Jenkins is prone to multiple vulnerabilities:
- Users who cached their CLI authentication would remain authenticated, because the fix for CVE-2019-1003004 does not reject existing remoting-based CLI authentication caches (CVE-2019-1003049)
- The f:validateButton form control for the Jenkins UI does not properly escape job URLs, resulting in a cross-site scripting (XSS) vulnerability exploitable by users with the ability to control job names (CVE-2019-1003050)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.164.2 LTS and < 2.172 Multiple Vulnerabilities - Windows`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.142270
Version used: 2021-08-31T08:01:19Z

References
cve: CVE-2019-1003049
cve: CVE-2019-1003050
url: https://jenkins.io/security/advisory/2019-04-10/
dfn-cert: DFN-CERT-2019-1326
dfn-cert: DFN-CERT-2019-0747

High (CVSS: 8.1)
NVT: Jenkins < 2.121 and < 2.107.3 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.121
Installation
path / port: /

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.121 or later / Jenkins LTS to 2.107.3 or later.

Affected Software/OS
Jenkins LTS up to and including 2.107.2, Jenkins weekly up to and including 2.120.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- An information exposure vulnerability in AboutJenkins.java, ListPluginsCommand.java that allows users with Overall/Read access to enumerate all installed plugins. (CVE-2018-1000192)
- An improper neutralization of control sequences vulnerability in HudsonPrivateSecurityRealm.java that allows users to sign up using user names containing control characters that can then appear to have the same name as other users, and cannot be deleted via the UI. (CVE-2018-1000193)
- A path traversal vulnerability in FilePath.java, SoloFilePathFilter.java that allows malicious agents to read and write arbitrary files on the Jenkins master, bypassing the agent-to-master security subsystem protection. (CVE-2018-1000194)
- A server-side request forgery vulnerability in ZipExtractionInstaller.java that allows users with Overall/Read permission to have Jenkins submit a HTTP GET request to an arbitrary URL and learn whether the response is successful (200) or not. (CVE-2018-1000195)

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

... continues on next page ...

... continued from previous page ...

Details: Jenkins < 2.121 and < 2.107.3 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.112298
Version used: 2022-06-15T03:04:08Z

References
cve: CVE-2018-1000192
cve: CVE-2018-1000193
cve: CVE-2018-1000194
cve: CVE-2018-1000195
url: https://jenkins.io/security/advisory/2018-05-09/

High (CVSS: 8.0)
NVT: Jenkins < 2.275, < 2.263.2 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.275
Installation
path / port: /

Impact
Successful exploitation would allow an attacker to:
- achieve stored and/or reflected cross-site scripting
- inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects when discarded by an administrator
- create symbolic links that allow them to access files outside workspaces using the workspace browser
- start up the application with unsafe legacy defaults after a restart
- check for the existence of XML files on the controller file system where the relative path can be constructed as 32 characters
- request or have legitimate Jenkins users request crafted URLs that rapidly use all available memory in Jenkins, potentially leading to out of memory errors
- access plugin-provided URLs without having the actual permissions to do so.

Solution:
Solution type: VendorFix
Update to version 2.275, 2.263.2 LTS or later.

Affected Software/OS
Jenkins version 2.274 and prior and 2.263.1 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:

... continues on next page ...

... continued from previous page ...

- Arbitrary file read vulnerability in workspace browsers (CVE-2021-21602)
- XSS vulnerability in notification bar (CVE-2021-21603)
- Improper handling of REST API XML deserialization errors (CVE-2021-21604)
- Path traversal vulnerability in agent names (CVE-2021-21605)
- Arbitrary file existence check in file fingerprints (CVE-2021-21606)
- Excessive memory allocation in graph URLs leads to denial of service (CVE-2021-21607)
- Stored XSS vulnerability in button labels (CVE-2021-21608)
- Missing permission check for paths with specific prefix (CVE-2021-21609)
- Reflected XSS vulnerability in markup formatter preview (CVE-2021-21610)
- Stored XSS vulnerability on new item page (CVE-2021-21611)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.275, < 2.263.2 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.112852
Version used: `2021-08-17T14:01:00Z`

References
`cve: CVE-2021-21602`
`cve: CVE-2021-21603`
`cve: CVE-2021-21604`
`cve: CVE-2021-21605`
`cve: CVE-2021-21606`
`cve: CVE-2021-21607`
`cve: CVE-2021-21608`
`cve: CVE-2021-21609`
`cve: CVE-2021-21610`
`cve: CVE-2021-21611`
`url: https://www.jenkins.io/security/advisory/2021-01-13/`
`dfn-cert: DFN-CERT-2021-0376`
`dfn-cert: DFN-CERT-2021-0102`

High (CVSS: 7.5)
NVT: Jenkins HTTP/2 DoS Vulnerability (CVE-2022-2048) - Windows

Summary
Jenkins is prone to an HTTP/2 denial of service (DoS) vulnerability in Jetty.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.363`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Update to version 2.361.1 (LTS), 2.363 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Jenkins version 2.346.3 (LTS) and prior and 2.362 and prior.

Vulnerability Insight
Jenkins bundles Winstone-Jetty, a wrapper around Jetty, to act as HTTP and servlet server when started using java -jar jenkins.war. This is how Jenkins is run when using any of the installers or packages, but not when run using servlet containers such as Tomcat.
Jenkins bundle versions of Jetty affected by the security vulnerability CVE-2022-2048. This vulnerability allows unauthenticated attackers to make the Jenkins UI unresponsive by exploiting Jetty's handling of invalid HTTP/2 requests, causing a denial of service.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins HTTP/2 DoS Vulnerability (CVE-2022-2048) - Windows`
OID:1.3.6.1.4.1.25623.1.0.148713
Version used: `2022-09-12T10:18:03Z`

References
`cve: CVE-2022-2048`
`url: https://www.jenkins.io/security/advisory/2022-09-09/`
`cert-bund: WID-SEC-2023-1017`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2023-0133`
`cert-bund: WID-SEC-2023-0027`
`cert-bund: WID-SEC-2022-1780`
`cert-bund: WID-SEC-2022-1778`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1766`
`cert-bund: WID-SEC-2022-1373`
`cert-bund: WID-SEC-2022-0614`
`dfn-cert: DFN-CERT-2023-0445`
`dfn-cert: DFN-CERT-2023-0112`
`dfn-cert: DFN-CERT-2023-0091`
`dfn-cert: DFN-CERT-2022-2708`
`dfn-cert: DFN-CERT-2022-1994`
`dfn-cert: DFN-CERT-2022-1706`

High (CVSS: 7.5)
NVT: Jenkins Multiple Vulnerabilities (Nov 2015) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`

... continues on next page ...

... continued from previous page ...

Fixed version: 1.638
Installation
path / port: /

Impact
Successful exploitation will allow remote attackers to obtain sensitive information, bypass the protection mechanism, gain elevated privileges, bypass intended access restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Jenkins main line users should update to 1.638, Jenkins LTS users should update to 1.625.2.

Affected Software/OS
All Jenkins main line releases up to and including 1.637, all Jenkins LTS releases up to and including 1.625.1.

Vulnerability Insight
Multiple flaws are due to:
- An error in 'Fingerprints' pages.
- The usage of publicly accessible salt to generate CSRF protection tokens.
- The XML external entity (XXE) vulnerability in the create-job CLI command.
- An improper verification of the shared secret used in JNLP slave connections.
- An error in sidepanel widgets in the CLI command overview and help pages.
- The directory traversal vulnerability in while requesting jnlpJars.
- An improper restriction on access to API tokens.
- The cross-site scripting vulnerability in the slave overview page.
- The unsafe deserialization in Jenkins remoting.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins Multiple Vulnerabilities (Nov 2015) - Windows
OID:1.3.6.1.4.1.25623.1.0.807001
Version used: 2023-05-18T09:08:59Z

References
cve: CVE-2015-5317
cve: CVE-2015-5318
cve: CVE-2015-5319
cve: CVE-2015-5320
cve: CVE-2015-5321
cve: CVE-2015-5322
cve: CVE-2015-5323
cve: CVE-2015-5324
cve: CVE-2015-5325
cve: CVE-2015-5326

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2015-8103
cve: CVE-2015-7536
cve: CVE-2015-7537
cve: CVE-2015-7538
cve: CVE-2015-7539
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://jenkins.io/security/advisory/2015-11-11/
url: http://www.securityfocus.com/bid/77572
url: http://www.securityfocus.com/bid/77570
url: http://www.securityfocus.com/bid/77574
url: http://www.securityfocus.com/bid/77636
url: http://www.securityfocus.com/bid/77619
url: https://jenkins.io/blog/2015/11/06/mitigating-unauthenticated-remote-code-e
↪xecution-0-day-in-jenkins-cli/
url: http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jen
↪kins-opennms-and-your-application-have-in-common-this-vulnerability
cert-bund: WID-SEC-2023-1215
cert-bund: CB-K16/0489
cert-bund: CB-K16/0141
cert-bund: CB-K15/1881
cert-bund: CB-K15/1672
cert-bund: CB-K15/1669
dfn-cert: DFN-CERT-2016-0531
dfn-cert: DFN-CERT-2016-0157
dfn-cert: DFN-CERT-2015-1985
dfn-cert: DFN-CERT-2015-1768
dfn-cert: DFN-CERT-2015-1761
```

High (CVSS: 7.5)
NVT: Jenkins < 2.289.2, < 2.300 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.637
Fixed version:     2.300
Installation
path / port:       /
```

Impact
Successful exploitation would allow an attacker to:
- cancel queue items and abort builds of jobs for which they have Item/Cancel permission even when they do not have Item/Read permission.
- use social engineering techniques to gain administrator access to Jenkins

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 2.300, 2.289.2 LTS or later.

Affected Software/OS
Jenkins version 2.299 and prior and 2.289.1 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-21670: Improper permission checks allow canceling queue items and aborting builds
- CVE-2021-21671: Session fixation

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.289.2, < 2.300 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.146202
Version used: `2021-08-17T14:01:00Z`

References
`url: https://www.jenkins.io/security/advisory/2021-06-30/`
`cve: CVE-2021-21670`
`cve: CVE-2021-21671`
`dfn-cert: DFN-CERT-2021-2216`
`dfn-cert: DFN-CERT-2021-2215`
`dfn-cert: DFN-CERT-2021-2028`
`dfn-cert: DFN-CERT-2021-1425`

High (CVSS: 7.5)
NVT: Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2566) - Windows

Summary
Jenkins is prone to an information disclosure vulnerability.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.356`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Update to version 2.356, 2.332.4 LTS or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Jenkins version 2.355 and prior and 2.332.3 LTS and prior.

Vulnerability Insight
An observable timing discrepancy on the login form allows distinguishing between login attempts with an invalid username, and login attempts with a valid username and wrong password, when using the Jenkins user database security realm. This allows attackers to determine the validity of attacker-specified usernames.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.148332
Version used: `2022-07-01T10:11:09Z`

References
`cve: CVE-2022-34174`
`url: https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2566`
`cert-bund: WID-SEC-2022-0445`
`dfn-cert: DFN-CERT-2023-0445`
`dfn-cert: DFN-CERT-2023-0388`
`dfn-cert: DFN-CERT-2023-0091`
`dfn-cert: DFN-CERT-2022-1408`

High (CVSS: 7.5)
NVT: Jenkins < 2.319.3, < 2.334 DoS Vulnerability - Windows

Summary
Jenkins is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.334`
`Installation`
`path / port: /`

Solution:
Solution type: VendorFix
Update to version 2.334, 2.319.3 LTS or later.

Affected Software/OS
Jenkins version 2.333 and prior and 2.319.2 LTS and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Jenkins is affected by the XStream library's vulnerability CVE-2021-43859. This library is used by Jenkins to serialize and deserialize various XML files, like global and job config.xml, build.xml, and numerous others.
This allows attackers able to submit crafted XML files to Jenkins to be parsed as configuration, e.g. through the POST config.xml API, to cause a denial of service (DoS).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.319.3, < 2.334 DoS Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.147622
Version used: `2022-02-10T14:05:57Z`

References
`cve: CVE-2021-43859`
`cve: CVE-2022-0538`
`url: https://www.jenkins.io/security/advisory/2022-02-09/`
`cert-bund: WID-SEC-2023-1017`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: WID-SEC-2022-1778`
`cert-bund: WID-SEC-2022-1772`
`cert-bund: WID-SEC-2022-1161`
`cert-bund: WID-SEC-2022-0756`
`cert-bund: WID-SEC-2022-0752`
`cert-bund: WID-SEC-2022-0729`
`cert-bund: WID-SEC-2022-0607`
`cert-bund: WID-SEC-2022-0530`
`dfn-cert: DFN-CERT-2023-1388`
`dfn-cert: DFN-CERT-2022-2305`
`dfn-cert: DFN-CERT-2022-1530`
`dfn-cert: DFN-CERT-2022-1469`
`dfn-cert: DFN-CERT-2022-0941`
`dfn-cert: DFN-CERT-2022-0322`
`dfn-cert: DFN-CERT-2022-0267`

High (CVSS: 7.5)
NVT: Jenkins < 2.186 and < 2.176.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.186`
`Installation path / port: /`

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 2.176.2 LTS, 2.186 weekly or later.

Affected Software/OS
Jenkins weekly up to and including 2.185 and Jenkins LTS up to and including 2.176.1

Vulnerability Insight
Jenkins is prone to multiple vulnerabilities:
- Arbitrary file write vulnerability using file parameter definitions (CVE-2019-10352)
- CSRF protection tokens does not expire (CVE-2019-10353)
- Unauthorized view fragment access (CVE-2019-10354)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.186 and < 2.176.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.142680
Version used: `2021-08-31T08:01:19Z`

References
`cve: CVE-2019-10352`
`cve: CVE-2019-10353`
`cve: CVE-2019-10354`
`url: https://jenkins.io/security/advisory/2019-07-17/`
`dfn-cert: DFN-CERT-2019-1469`

High (CVSS: 7.5)
NVT: Jenkins < 2.133 and < 2.121.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.133
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.132 or later / Jenkins LTS to 2.121.2 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Jenkins LTS up to and including 2.121.1, Jenkins weekly up to and including 2.132.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Users without Overall/Read permission can have Jenkins reset parts of global configuration on the next restart (CVE-2018-1999001).
- Arbitrary file read vulnerability (CVE-2018-1999002).
- Unauthorized users could cancel queued builds (CVE-2018-1999003).
- Unauthorized users could initiate and abort agent launches (CVE-2018-1999004).
- Stored XSS vulnerability (CVE-2018-1999005).
- Unauthorized users are able to determine when a plugin was extracted from its JPI package (CVE-2018-1999006).
- XSS vulnerability in Stapler debug mode (CVE-2018-1999007).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.133 and < 2.121.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.112332
Version used: `2022-06-15T03:04:08Z`

References
`cve: CVE-2018-1999001`
`cve: CVE-2018-1999002`
`cve: CVE-2018-1999003`
`cve: CVE-2018-1999004`
`cve: CVE-2018-1999005`
`cve: CVE-2018-1999006`
`cve: CVE-2018-1999007`
`url: https://jenkins.io/security/advisory/2018-07-18/`
`dfn-cert: DFN-CERT-2018-1419`

High (CVSS: 7.4)
NVT: Jenkins Multiple Vulnerabilities (May 2016) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.3
Installation
path / port:       /
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to obtain sensitive information, bypass the protection mechanism, gain elevated privileges, bypass intended access restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Jenkins main line users should update to 2.3, Jenkins LTS users should update to 1.651.2.

Affected Software/OS
All Jenkins main line releases up to and including 2.2, All Jenkins LTS releases up to and including 1.651.1.

Vulnerability Insight
Multiple flaws are due to:
- The XML/JSON API endpoints providing information about installed plugins were missing permissions checks, allowing any user with read access to Jenkins to determine which plugins and versions were installed.
- The users with extended read access could access encrypted secrets stored directly in the configuration of those items.
- A missing permissions check allowed any user with access to Jenkins to trigger an update of update site metadata. This could be combined with DNS cache poisoning to disrupt Jenkins service.
- The Some Jenkins URLs did not properly validate the redirect URLs, which allowed malicious users to create URLs that redirect users to arbitrary scheme-relative URLs.
- The API URL /computer/(master)/api/xml allowed users with the 'extended read' permission for the master node to see some global Jenkins configuration, including the configuration of the security realm.
- By changing the freely editable 'full name', malicious users with multiple user accounts could prevent other users from logging in, as 'full name' was resolved before actual user name to determine which account is currently trying to log in.
- An improper validation of build parameters in Jenkins.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins Multiple Vulnerabilities (May 2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.807329
Version used: `2021-10-12T08:01:25Z`

References
`cve: CVE-2016-3721`
`cve: CVE-2016-3722`
`cve: CVE-2016-3723`
`cve: CVE-2016-3724`
`cve: CVE-2016-3725`
`cve: CVE-2016-3726`
`cve: CVE-2016-3727`

... continues on next page ...

... continued from previous page ...

url: https://jenkins.io/security/advisory/2016-05-11/
cert-bund: CB-K16/1303
cert-bund: CB-K16/0714
dfn-cert: DFN-CERT-2016-1386
dfn-cert: DFN-CERT-2016-0770

High (CVSS: 7.3)
NVT: Jenkins Multiple Vulnerabilities (Nov 2017) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.89
Installation
path / port: /

Impact
Successful exploitation will allow remote attackers to affect the integrity of the application.

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.89 or later / Jenkins LTS to 2.73.3 or later.

Affected Software/OS
Jenkins LTS 2.73.2 and prior, Jenkins weekly up to and including 2.88.

Vulnerability Insight
Multiple flaws are due to:
- unsafe use of user names as directory names
- a persisted XSS vulnerability in autocompletion suggestions

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins Multiple Vulnerabilities (Nov 2017) - Windows
OID:1.3.6.1.4.1.25623.1.0.112131
Version used: 2023-07-14T16:09:27Z

References
cve: CVE-2017-1000391
cve: CVE-2017-1000392
url: https://jenkins.io/security/advisory/2017-11-08/

High (CVSS: 7.2)
NVT: Jenkins < 2.160 and < 2.150.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.637`
`Fixed version: 2.160`
`Installation path / port: /`

Solution:
Solution type: VendorFix
Upgrade Jenkins weekly to 2.160 or later / Jenkins LTS to 2.150.2 or later.

Affected Software/OS
Jenkins LTS through 2.150.1, Jenkins weekly through 2.159.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Administrators could persist access to Jenkins using crafted 'Remember me' cookie (CVE-2019-1003003).
- Deleting a user in an external security realm did not invalidate their session or 'Remember me' cookie (CVE-2019-1003004).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.160 and < 2.150.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.112495
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2019-1003003`
`cve: CVE-2019-1003004`
`url: https://jenkins.io/security/advisory/2019-01-16/`

[return to 10.0.0.21]

2.1.5 High 22/tcp

High (CVSS: 9.8)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)

Product detection result
`cpe:/a:openbsd:openssh:7.1`

... continues on next page ...

... continued from previous page ...

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.1
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 Windows

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 (Windows)
OID:1.3.6.1.4.1.25623.1.0.810768
Version used: 2023-07-14T16:09:27Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2016-1908
url: http://openwall.com/lists/oss-security/2016/01/15/13
url: http://www.securityfocus.com/bid/84427
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4

... continues on next page ...

... continued from previous page ...

```
url: http://www.openssh.com/txt/release-7.2
url: https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0
↪db113c71e234416c
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741
cert-bund: CB-K16/1485
cert-bund: CB-K16/0694
cert-bund: CB-K16/0684
cert-bund: CB-K16/0449
cert-bund: CB-K16/0162
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-0754
dfn-cert: DFN-CERT-2016-0733
dfn-cert: DFN-CERT-2016-0488
dfn-cert: DFN-CERT-2016-0182
```

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`vagrant:vagrant`

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

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

Vulnerability Insight
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2023-05-26T09:09:36Z`

... continues on next page ...

... continued from previous page ...

References
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2023-1944

High (CVSS: 7.5)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)

Product detection result
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
openssh is prone to denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result
Installed version: 7.1
Fixed version: 7.3
Installation
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 Windows

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.809121
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2016-6515
cve: CVE-2016-6210
url: http://www.openssh.com/txt/release-7.3
url: http://www.securityfocus.com/bid/92212
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
cert-bund: WID-SEC-2023-0450
cert-bund: WID-SEC-2023-0449
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1753
cert-bund: CB-K17/1349
cert-bund: CB-K17/1292
cert-bund: CB-K17/0055
cert-bund: CB-K16/1837
cert-bund: CB-K16/1629
cert-bund: CB-K16/1487
cert-bund: CB-K16/1485
cert-bund: CB-K16/1252
cert-bund: CB-K16/1221
cert-bund: CB-K16/1082
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1407
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1943

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1729
dfn-cert: DFN-CERT-2016-1576
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-1331
dfn-cert: DFN-CERT-2016-1243
dfn-cert: DFN-CERT-2016-1149

High (CVSS: 7.3)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Windows)

Product detection result
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
openssh is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.1
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 Windows.

Vulnerability Insight
Multiple flaws exist due to:
- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.
- 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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH Multiple Vulnerabilities Jan17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.810325
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2016-10009
cve: CVE-2016-10010
cve: CVE-2016-10011
cve: CVE-2016-10012
cve: CVE-2016-10708
url: https://www.openssh.com/txt/release-7.4
url: http://www.securityfocus.com/bid/94968
url: http://www.securityfocus.com/bid/94972
url: http://www.securityfocus.com/bid/94977
url: http://www.securityfocus.com/bid/94975
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=28652bca29046f62c7045e93
↪3e6b931de1d16737
cert-bund: CB-K18/0919
cert-bund: CB-K18/0591
cert-bund: CB-K18/0137
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1292
cert-bund: CB-K17/1061
cert-bund: CB-K17/0527
cert-bund: CB-K17/0377
cert-bund: CB-K17/0127
cert-bund: CB-K17/0041
cert-bund: CB-K16/1991
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-1432
dfn-cert: DFN-CERT-2018-1112
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-1068
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-1096
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0386
dfn-cert: DFN-CERT-2017-0130
dfn-cert: DFN-CERT-2017-0042
dfn-cert: DFN-CERT-2016-2099
```

[return to 10.0.0.21]

2.1.6 High 8585/tcp

High (CVSS: 10.0)
NVT: PHP End Of Life Detection (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (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:5.3.10
Installed version: 5.3.10
EOL version:       5.3
EOL date:          2014-08-14
```

Impact

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

Solution:

Solution type: VendorFix

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP End Of Life Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.105888
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: https://secure.php.net/supported-versions.php`
`url: https://secure.php.net/eol.php`

High (CVSS: 10.0)
NVT: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.3.15/5.4.5`

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to PHP 5.4.5 or 5.3.15 or later.

Affected Software/OS
PHP version before 5.3.15 and 5.4.x before 5.4.5

Vulnerability Insight
Flaw related to overflow in the _php_stream_scandir function in the stream implementation.

Vulnerability Detection Method
Details: PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803317
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-2688
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/54638
url: http://en.securitylab.ru/nvd/427456.php
url: http://secunia.com/advisories/cve_reference/CVE-2012-2688
cert-bund: CB-K13/1037
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2013-2065
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-0357
dfn-cert: DFN-CERT-2012-1655
dfn-cert: DFN-CERT-2012-1654
dfn-cert: DFN-CERT-2012-1560
dfn-cert: DFN-CERT-2012-1541
dfn-cert: DFN-CERT-2012-1505
dfn-cert: DFN-CERT-2012-1504
dfn-cert: DFN-CERT-2012-1503
dfn-cert: DFN-CERT-2012-1499
dfn-cert: DFN-CERT-2012-1422

High (CVSS: 10.0)
NVT: PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: N/A

Impact
Successful exploitation could allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial of service conditions.

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 Version 5.4.3 and prior on Windows

Vulnerability Insight
The flaw is due to an error in the 'com_print_typeinfo()' function, which allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types.

Vulnerability Detection Method
Details: PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.902836
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-2376
url: http://www.securityfocus.com/bid/53621

... continues on next page ...

... continued from previous page ...

url: http://www.exploit-db.com/exploits/18861
url: http://isc.sans.edu/diary.html?storyid=13255
url: https://bugzilla.redhat.com/show_bug.cgi?id=823464
url: http://openwall.com/lists/oss-security/2012/05/20/2
url: http://packetstormsecurity.org/files/112851/php54-exec.txt

High (CVSS: 10.0)
NVT: Apache HTTP Server End of Life (EOL) Detection (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
The Apache HTTP Server version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result
The "Apache HTTP Server" version on the remote host has reached the end of life.
CPE: cpe:/a:apache:http_server:2.2.21
Installed version: 2.2.21
Location/URL: 8585/tcp
EOL version: 2.2
EOL date: 2017-12-31

Impact
An EOL version of the Apache HTTP Server 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 Apache HTTP Server version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: Apache HTTP Server End of Life (EOL) Detection (Windows)
OID:1.3.6.1.4.1.25623.1.0.108135
Version used: 2021-03-02T10:48:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.117232)

References
url: https://archive.apache.org/dist/httpd/Announcement1.3.html
url: https://archive.apache.org/dist/httpd/Announcement2.0.html
url: https://www.apache.org/dist/httpd/Announcement2.2.html
url: https://en.wikipedia.org/wiki/Apache_HTTP_Server#Versions

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 03 - Jul16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

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

Vulnerability Insight
Multiple flaws exist 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.

... continues on next page ...

... continued from previous page ...

- The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures.
- An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script.
- An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 03 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808602
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-4537`
`cve: CVE-2016-4538`
`cve: CVE-2016-4539`
`cve: CVE-2016-4540`
`cve: CVE-2016-4541`
`cve: CVE-2016-4542`
`cve: CVE-2016-4543`
`cve: CVE-2016-4544`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/89844`
`url: http://www.securityfocus.com/bid/90172`
`url: http://www.securityfocus.com/bid/90173`
`url: http://www.securityfocus.com/bid/90174`
`url: http://www.php.net/ChangeLog-7.php`
`cert-bund: CB-K16/1776`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K16/0912`
`cert-bund: CB-K16/0909`
`cert-bund: CB-K16/0868`
`cert-bund: CB-K16/0779`
`cert-bund: CB-K16/0774`
`cert-bund: CB-K16/0760`
`dfn-cert: DFN-CERT-2016-1882`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2016-0972`
`dfn-cert: DFN-CERT-2016-0960`
`dfn-cert: DFN-CERT-2016-0924`
`dfn-cert: DFN-CERT-2016-0835`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0827
dfn-cert: DFN-CERT-2016-0814

High (CVSS: 9.8)
NVT: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Windows

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.4.54
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.54 or later.

Affected Software/OS
Apache HTTP Server version 2.4.53 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-26377: mod_proxy_ajp: Possible request smuggling
- CVE-2022-28330: Read beyond bounds in mod_isapi
- CVE-2022-28614: Read beyond bounds via ap_rwrite()
- CVE-2022-28615: Read beyond bounds in ap_strcmp_match()
- CVE-2022-29404: Denial of service in mod_lua r:parsebody
- CVE-2022-30556: Information disclosure in mod_lua with websockets
- CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.148253
Version used: 2022-06-20T03:04:15Z

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

cve: CVE-2022-26377
cve: CVE-2022-28330
cve: CVE-2022-28614
cve: CVE-2022-28615
cve: CVE-2022-29404
cve: CVE-2022-30556
cve: CVE-2022-31813
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54
cert-bund: WID-SEC-2023-0134
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1766
cert-bund: WID-SEC-2022-1764
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0192
cert-bund: CB-K22/0692
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2789
dfn-cert: DFN-CERT-2022-2652
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2310
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1833
dfn-cert: DFN-CERT-2022-1720
dfn-cert: DFN-CERT-2022-1353
dfn-cert: DFN-CERT-2022-1296

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)

Product detection result

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to PHP version 5.6.25, or 7.0.10, or later.

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 02 - Sep16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809318
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-7124`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-7125
cve: CVE-2016-7126
cve: CVE-2016-7127
cve: CVE-2016-7128
cve: CVE-2016-7129
cve: CVE-2016-7130
cve: CVE-2016-7131
cve: CVE-2016-7132
url: http://www.php.net/ChangeLog-7.php
url: http://www.securityfocus.com/bid/92756
url: http://www.securityfocus.com/bid/92552
url: http://www.securityfocus.com/bid/92755
url: http://www.securityfocus.com/bid/92757
url: http://www.securityfocus.com/bid/92564
url: http://www.securityfocus.com/bid/92758
url: http://www.php.net/ChangeLog-5.php
cert-bund: CB-K16/1776
cert-bund: CB-K16/1772
cert-bund: CB-K16/1549
cert-bund: CB-K16/1543
cert-bund: CB-K16/1532
cert-bund: CB-K16/1499
cert-bund: CB-K16/1440
cert-bund: CB-K16/1280
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1878
dfn-cert: DFN-CERT-2016-1641
dfn-cert: DFN-CERT-2016-1639
dfn-cert: DFN-CERT-2016-1631
dfn-cert: DFN-CERT-2016-1590
dfn-cert: DFN-CERT-2016-1526
dfn-cert: DFN-CERT-2016-1359
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3.10
```

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - 02 - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808789
Version used: 2022-07-22T10:11:18Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-5771
cve: CVE-2016-5770
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/91401
url: http://www.securityfocus.com/bid/91403
cert-bund: CB-K16/2012
cert-bund: CB-K16/1776
cert-bund: CB-K16/1452
cert-bund: CB-K16/1179
cert-bund: CB-K16/1106
cert-bund: CB-K16/1070
cert-bund: CB-K16/1030

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0965
dfn-cert: DFN-CERT-2018-0576
dfn-cert: DFN-CERT-2016-2125
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1541
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1178
dfn-cert: DFN-CERT-2016-1139
dfn-cert: DFN-CERT-2016-1097
dfn-cert: DFN-CERT-2016-1022
```

High (CVSS: 9.8)
NVT: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows

Product detection result

```
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

Apache HTTP Server is prone to a buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 2.2.21
Fixed version:     2.4.52
Installation
path / port:       8585/tcp
```

Solution:

Solution type: VendorFix

Update to version 2.4.52 or later.

Affected Software/OS

Apache HTTP Server versions through 2.4.51.

Vulnerability Insight

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Vulnerability Detection Method

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

Details: `Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.117857

Version used: `2021-12-23T12:12:57Z`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2021-44790
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0727
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0190
cert-bund: CB-K22/0619
cert-bund: CB-K21/1296
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0192
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2656

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.5.34

Impact

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808198
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-4070`
`cve: CVE-2016-4071`
`cve: CVE-2016-4072`
`cve: CVE-2016-4073`
`cve: CVE-2015-8865`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/85800`
`url: http://www.securityfocus.com/bid/85801`
`url: http://www.securityfocus.com/bid/85802`
`url: http://www.securityfocus.com/bid/85991`
`url: http://www.securityfocus.com/bid/85993`
`url: http://www.php.net/ChangeLog-7.php`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1776
cert-bund: CB-K16/1319
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0884
cert-bund: CB-K16/0872
cert-bund: CB-K16/0779
cert-bund: CB-K16/0723
cert-bund: CB-K16/0705
cert-bund: CB-K16/0614
cert-bund: CB-K16/0494
dfn-cert: DFN-CERT-2018-1161
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1402
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0940
dfn-cert: DFN-CERT-2016-0929
dfn-cert: DFN-CERT-2016-0835
dfn-cert: DFN-CERT-2016-0775
dfn-cert: DFN-CERT-2016-0764
dfn-cert: DFN-CERT-2016-0659
dfn-cert: DFN-CERT-2016-0536
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808787
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-5773`
`cve: CVE-2016-5772`
`cve: CVE-2016-5769`
`cve: CVE-2016-5768`
`cve: CVE-2016-5766`
`cve: CVE-2016-5767`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/91397`
`url: http://www.securityfocus.com/bid/91398`
`url: http://www.securityfocus.com/bid/91399`
`url: http://www.securityfocus.com/bid/91396`
`url: http://www.securityfocus.com/bid/91395`
`url: http://www.php.net/ChangeLog-7.php`
`cert-bund: CB-K17/1575`
`cert-bund: CB-K17/1461`
`cert-bund: CB-K17/1252`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1868
cert-bund: CB-K16/1776
cert-bund: CB-K16/1722
cert-bund: CB-K16/1629
cert-bund: CB-K16/1600
cert-bund: CB-K16/1452
cert-bund: CB-K16/1257
cert-bund: CB-K16/1230
cert-bund: CB-K16/1179
cert-bund: CB-K16/1115
cert-bund: CB-K16/1106
cert-bund: CB-K16/1077
cert-bund: CB-K16/1070
cert-bund: CB-K16/1045
cert-bund: CB-K16/1030
cert-bund: CB-K16/0975
cert-bund: CB-K16/0966
cert-bund: CB-K16/0965
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2741
dfn-cert: DFN-CERT-2018-0576
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2016-1974
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1822
dfn-cert: DFN-CERT-2016-1729
dfn-cert: DFN-CERT-2016-1697
dfn-cert: DFN-CERT-2016-1541
dfn-cert: DFN-CERT-2016-1335
dfn-cert: DFN-CERT-2016-1295
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1184
dfn-cert: DFN-CERT-2016-1178
dfn-cert: DFN-CERT-2016-1144
dfn-cert: DFN-CERT-2016-1139
dfn-cert: DFN-CERT-2016-1110
dfn-cert: DFN-CERT-2016-1097
dfn-cert: DFN-CERT-2016-1033
dfn-cert: DFN-CERT-2016-1022
dfn-cert: DFN-CERT-2016-1021
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 01 - Apr16 (Windows)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.33 or 5.6.19 or later.

Affected Software/OS
PHP versions before 5.5.33, and 5.6.x before 5.6.19 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - 01 - Apr16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.807806
Version used: 2021-10-12T10:01:28Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-3142
cve: CVE-2016-3141
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
cert-bund: CB-K16/1776

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1620
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0723
cert-bund: CB-K16/0623
cert-bund: CB-K16/0614
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1717
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0775
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0659
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Nov 2016) - Windows

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     5.6.28
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.28, 7.0.13 or later.

Affected Software/OS
PHP versions before 5.6.28 and 7.x before 7.0.13.

Vulnerability Insight
The following flaws exist:
- CVE-2016-8670: Stack Buffer Overflow in GD dynamicGetbuf
- CVE-2016-9933, CVE-2016-9934: Multiple denial of service (DoS) vulnerabilities
- CVE-2016-10397: Security bypass vulnerability

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 (Nov 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.811488
Version used: 2021-11-25T14:03:32Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-8670
cve: CVE-2016-9933
cve: CVE-2016-9934
cve: CVE-2016-10397
url: http://www.php.net/ChangeLog-5.php
url: http://www.php.net/ChangeLog-7.php
url: http://bugs.php.net/73280
url: http://bugs.php.net/72696
url: http://bugs.php.net/73331
url: http://bugs.php.net/73192
cert-bund: CB-K17/1575
cert-bund: CB-K17/1461
cert-bund: CB-K17/1358
cert-bund: CB-K17/1252
cert-bund: CB-K17/0269
cert-bund: CB-K17/0124
cert-bund: CB-K17/0053
cert-bund: CB-K17/0015
cert-bund: CB-K16/2015
cert-bund: CB-K16/2011
cert-bund: CB-K16/1943
cert-bund: CB-K16/1790
cert-bund: CB-K16/1606
dfn-cert: DFN-CERT-2019-2707
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2017-0274
dfn-cert: DFN-CERT-2017-0131
dfn-cert: DFN-CERT-2017-0058
dfn-cert: DFN-CERT-2017-0016
dfn-cert: DFN-CERT-2016-2130
dfn-cert: DFN-CERT-2016-2123
dfn-cert: DFN-CERT-2016-2053

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1887
dfn-cert: DFN-CERT-2016-1704

High (CVSS: 9.8)
NVT: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.4.53
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.53 or later.

Affected Software/OS
Apache HTTP Server version 2.4.52 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody
- CVE-2022-22720: HTTP request smuggling vulnerability
- CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody
- CVE-2022-23943: mod_sed: Read/write beyond bounds

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.113838
Version used: 2022-03-21T03:03:41Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2022-22719
cve: CVE-2022-22720
cve: CVE-2022-22721
cve: CVE-2022-23943
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0898
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0646
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0290
cert-bund: CB-K22/0619
cert-bund: CB-K22/0306
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0678
dfn-cert: DFN-CERT-2022-0582

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Jul 2017 - 01) - Windows

Product detection result

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (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: 5.3.10
Fixed version:     5.6.31
Installation
path / port:       8585/tcp
```

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

Solution:
Solution type: VendorFix
Update to 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 the '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.
- Heap buffer overread (READ: 1) finish_nested_data from unserialize
- Add oniguruma upstream fix

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities (Jul 2017 - 01) - Windows`
OID:1.3.6.1.4.1.25623.1.0.811481
Version used: `2022-07-22T10:11:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-7890`
`cve: CVE-2017-9224`
`cve: CVE-2017-9225`
`cve: CVE-2017-9226`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-9227
cve: CVE-2017-9228
cve: CVE-2017-9229
cve: CVE-2017-11144
cve: CVE-2017-11145
cve: CVE-2017-11628
cve: CVE-2017-12933
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/99492
url: http://www.securityfocus.com/bid/99550
url: http://www.securityfocus.com/bid/99605
url: http://www.securityfocus.com/bid/99612
url: http://www.securityfocus.com/bid/99489
url: http://www.php.net/ChangeLog-7.php
cert-bund: CB-K18/0270
cert-bund: CB-K18/0048
cert-bund: CB-K17/2123
cert-bund: CB-K17/1575
cert-bund: CB-K17/1573
cert-bund: CB-K17/1562
cert-bund: CB-K17/1468
cert-bund: CB-K17/1461
cert-bund: CB-K17/1373
cert-bund: CB-K17/1358
cert-bund: CB-K17/1132
cert-bund: CB-K17/1011
cert-bund: CB-K17/0908
dfn-cert: DFN-CERT-2020-1221
dfn-cert: DFN-CERT-2020-0484
dfn-cert: DFN-CERT-2020-0479
dfn-cert: DFN-CERT-2019-1052
dfn-cert: DFN-CERT-2018-2116
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0290
dfn-cert: DFN-CERT-2018-0055
dfn-cert: DFN-CERT-2017-2219
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1644
dfn-cert: DFN-CERT-2017-1629
dfn-cert: DFN-CERT-2017-1530
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1432
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1161
dfn-cert: DFN-CERT-2017-1046
dfn-cert: DFN-CERT-2017-0932
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Jan 2017 - 02) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.30
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to 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
The following flaws exist:
- Fixed bug #73825 (Heap out of bounds read on unserialize in finish_nested_data()). (CVE-2016-10161)
- Fixed bug #73737 (FPE when parsing a tag format). (CVE-2016-10158)
- Fixed bug #73869 (Signed Integer Overflow gd_io.c). (CVE-2016-10168)
- Fixed bug #73868 (DOS vulnerability in gdImageCreateFromGd2Ctx()). (CVE-2016-10167)
- Fixed bug #73773 (Seg fault when loading hostile phar). (CVE-2017-11147)
- Fixed bug #73768 (Memory corruption when loading hostile phar). (CVE-2016-10160)
- Fixed bug #73764 (Crash while loading hostile phar archive). (CVE-2016-10159)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities (Jan 2017 - 02) - Windows
OID:1.3.6.1.4.1.25623.1.0.108053
Version used: 2022-07-22T10:11:18Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
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: CVE-2016-10158
cve: CVE-2016-10168
cve: CVE-2016-10167
cve: CVE-2017-11147
cve: CVE-2016-10160
cve: CVE-2016-10159
url: http://www.php.net/ChangeLog-5.php
url: http://www.php.net/ChangeLog-7.php
url: http://bugs.php.net/73825
url: http://bugs.php.net/73737
url: http://bugs.php.net/73869
url: http://bugs.php.net/73868
url: http://bugs.php.net/73773
url: http://bugs.php.net/73768
url: http://bugs.php.net/73764
cert-bund: CB-K17/1957
cert-bund: CB-K17/1575
cert-bund: CB-K17/1461
cert-bund: CB-K17/1358
cert-bund: CB-K17/1252
cert-bund: CB-K17/0527
cert-bund: CB-K17/0327
cert-bund: CB-K17/0318
cert-bund: CB-K17/0269
cert-bund: CB-K17/0264
cert-bund: CB-K17/0232
cert-bund: CB-K17/0182
cert-bund: CB-K17/0141
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2017-2044
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0334
dfn-cert: DFN-CERT-2017-0325
dfn-cert: DFN-CERT-2017-0274
dfn-cert: DFN-CERT-2017-0270
dfn-cert: DFN-CERT-2017-0234
dfn-cert: DFN-CERT-2017-0179
dfn-cert: DFN-CERT-2017-0144

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Feb 2019) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.40
Installation
path / port: 8585/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
The following flaws exist:
- Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166)
- Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977)
- Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023)
- Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023)
- Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023)
- Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023)
- Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023)
- Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023)
- Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023)
- Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021)
- Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020)
- Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities (Feb 2019) - Windows
OID:1.3.6.1.4.1.25623.1.0.142049
Version used: 2021-11-26T13:39:39Z

. . . continues on next page . . .

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-10166
cve: CVE-2019-9020
cve: CVE-2019-9021
cve: CVE-2019-9023
cve: CVE-2019-9024
cve: CVE-2019-6977
url: http://www.php.net/ChangeLog-5.php
url: http://www.php.net/ChangeLog-7.php
url: https://bugs.php.net/bug.php?id=77269
url: https://bugs.php.net/bug.php?id=77270
url: https://bugs.php.net/bug.php?id=77370
url: https://bugs.php.net/bug.php?id=77371
url: https://bugs.php.net/bug.php?id=77381
url: https://bugs.php.net/bug.php?id=77382
url: https://bugs.php.net/bug.php?id=77385
url: https://bugs.php.net/bug.php?id=77394
url: https://bugs.php.net/bug.php?id=77418
url: https://bugs.php.net/bug.php?id=77247
url: https://bugs.php.net/bug.php?id=77242
url: https://bugs.php.net/bug.php?id=77380
cert-bund: WID-SEC-2022-2127
cert-bund: CB-K19/0166
cert-bund: CB-K17/1252
cert-bund: CB-K17/0318
cert-bund: CB-K17/0232
cert-bund: CB-K17/0182
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2020-2398
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0898
dfn-cert: DFN-CERT-2020-0680
dfn-cert: DFN-CERT-2019-2283
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2019-1181
dfn-cert: DFN-CERT-2019-0804
dfn-cert: DFN-CERT-2019-0698
dfn-cert: DFN-CERT-2019-0434
dfn-cert: DFN-CERT-2019-0368
dfn-cert: DFN-CERT-2019-0313

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-0241
dfn-cert: DFN-CERT-2019-0212
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2017-0325
dfn-cert: DFN-CERT-2017-0234
dfn-cert: DFN-CERT-2017-0179

High (CVSS: 9.8)
NVT: PHP Multiple DoS Vulnerabilities (Oct 2016) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.27
Installation
path / port: 8585/tcp

Impact
Successfully exploiting this issue allows a remote attacker to cause a DoS, or possibly have unspecified other impact.

Solution:
Solution type: VendorFix
Update to version 5.6.27, 7.0.12 or later.

Affected Software/OS
PHP versions before 5.6.27 and 7.0.x through 7.0.11.

Vulnerability Insight
- Fixed bug #73003 (Integer Overflow in gdImageWebpCtx of gd_webp.c).
- Fixed bug #73147 (Use After Free in PHP7 unserialize()).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple DoS Vulnerabilities (Oct 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809337
Version used: 2022-04-13T13:17:10Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-7568
cve: CVE-2016-9137
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/93184
url: http://www.securityfocus.com/bid/93577
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: https://bugs.php.net/bug.php?id=73147
cert-bund: CB-K17/0327
cert-bund: CB-K17/0269
cert-bund: CB-K16/1941
cert-bund: CB-K16/1868
cert-bund: CB-K16/1854
cert-bund: CB-K16/1811
cert-bund: CB-K16/1645
cert-bund: CB-K16/1606
cert-bund: CB-K16/1603
dfn-cert: DFN-CERT-2017-0334
dfn-cert: DFN-CERT-2017-0274
dfn-cert: DFN-CERT-2016-2047
dfn-cert: DFN-CERT-2016-1974
dfn-cert: DFN-CERT-2016-1961
dfn-cert: DFN-CERT-2016-1918
dfn-cert: DFN-CERT-2016-1745
dfn-cert: DFN-CERT-2016-1704
dfn-cert: DFN-CERT-2016-1700

High (CVSS: 9.8)
NVT: Apache HTTP Server Multiple Vulnerabilities June17 (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.2.33
Installation
path / port: 8585/tcp

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

Solution:
Solution type: VendorFix
Update 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.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Multiple Vulnerabilities June17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.811213
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2017-7679
cve: CVE-2017-3169
cve: CVE-2017-3167
url: http://seclists.org/oss-sec/2017/q2/509
url: http://www.securityfocus.com/bid/99135

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/99134
url: http://httpd.apache.org/security/vulnerabilities_24.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/0066
cert-bund: CB-K17/2188
cert-bund: CB-K17/2013
cert-bund: CB-K17/1936
cert-bund: CB-K17/1854
cert-bund: CB-K17/1842
cert-bund: CB-K17/1768
cert-bund: CB-K17/1747
cert-bund: CB-K17/1622
cert-bund: CB-K17/1382
cert-bund: CB-K17/1279
cert-bund: CB-K17/1154
cert-bund: CB-K17/1023
dfn-cert: DFN-CERT-2019-0358
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2290
dfn-cert: DFN-CERT-2017-2104
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1843
dfn-cert: DFN-CERT-2017-1828
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1327
dfn-cert: DFN-CERT-2017-1193
dfn-cert: DFN-CERT-2017-1058
```

High (CVSS: 9.8)
NVT: PHP Directory Traversal Vulnerability - Jul16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a directory traversal vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Directory Traversal Vulnerability - Jul16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808616
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2014-9767
cve: CVE-2015-6834
cve: CVE-2015-6835
cve: CVE-2015-6837
cve: CVE-2015-6838
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/76652
url: http://www.securityfocus.com/bid/76649
url: http://www.securityfocus.com/bid/76733
url: http://www.securityfocus.com/bid/76734
url: http://www.securityfocus.com/bid/76738

... continues on next page ...

... continued from previous page ...

```
url: http://www.openwall.com/lists/oss-security/2016/03/16/20
cert-bund: CB-K16/1776
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0623
cert-bund: CB-K16/0614
cert-bund: CB-K16/0422
cert-bund: CB-K15/1571
cert-bund: CB-K15/1561
cert-bund: CB-K15/1478
cert-bund: CB-K15/1439
cert-bund: CB-K15/1415
cert-bund: CB-K15/1337
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0659
dfn-cert: DFN-CERT-2016-0460
dfn-cert: DFN-CERT-2015-1658
dfn-cert: DFN-CERT-2015-1644
dfn-cert: DFN-CERT-2015-1556
dfn-cert: DFN-CERT-2015-1515
dfn-cert: DFN-CERT-2015-1493
dfn-cert: DFN-CERT-2015-1407
```

High (CVSS: 9.8)
NVT: PHP < 7.0.12 RCE / DoS Vulnerability - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     7.0.12
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.0.12 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions prior to 7.0.12.

Vulnerability Insight
The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.0.12 RCE / DoS Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.117801
Version used: `2022-07-22T10:11:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
cve: CVE-2016-7480
url: https://www.php.net/ChangeLog-7.php#7.0.12
url: https://bugs.php.net/bug.php?id=73257
url: http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-
↪vulnerabilities-web-programming-language-php-7
cert-bund: CB-K17/0318
dfn-cert: DFN-CERT-2017-0325
```

High (CVSS: 9.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP is prone to denial of service and unspecified vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     5.5.32
```

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808606
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-4342`
`cve: CVE-2016-2554`
`url: http://www.php.net/ChangeLog-7.php`
`url: http://www.securityfocus.com/bid/89154`
`url: http://www.securityfocus.com/bid/83353`
`url: http://www.openwall.com/lists/oss-security/2016/04/28/2`
`cert-bund: CB-K16/1776`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K16/0912`
`cert-bund: CB-K16/0868`
`cert-bund: CB-K16/0779`
`cert-bund: CB-K16/0760`
`cert-bund: CB-K16/0623`
`cert-bund: CB-K16/0614`
`cert-bund: CB-K16/0405`
`dfn-cert: DFN-CERT-2016-1882`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2016-0972`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0924
dfn-cert: DFN-CERT-2016-0835
dfn-cert: DFN-CERT-2016-0814
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0659
dfn-cert: DFN-CERT-2016-0441

High (CVSS: 9.8)
NVT: PHP Arbitrary Code Execution Vulnerability - Aug16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.27, or 5.6.11, or later.

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Arbitrary Code Execution Vulnerability - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808670
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10

... continues on next page ...

... continued from previous page ...

Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-4116
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/75127
cert-bund: CB-K16/1179
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0911
cert-bund: CB-K16/0868
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0944
dfn-cert: DFN-CERT-2016-0924

High (CVSS: 9.8)
NVT: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP released new versions which include a security fix.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.4.28
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.4.28, 8.0.16, 8.1.3 or later.

Affected Software/OS
PHP prior to version 7.4.28, 8.0.x through 8.0.15 and 8.1.x through 8.1.2.

Vulnerability Insight
Fix #81708: UAF due to php_filter_float() failing for ints.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows
OID:1.3.6.1.4.1.25623.1.0.147658
Version used: 2022-09-30T10:11:44Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21708
url: https://www.php.net/ChangeLog-7.php#7.4.28
url: https://www.php.net/ChangeLog-8.php#8.0.16
url: https://www.php.net/ChangeLog-8.php#8.1.3
url: https://bugs.php.net/bug.php?id=81708
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0280
cert-bund: CB-K22/0201
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2500
dfn-cert: DFN-CERT-2022-2499
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0407
dfn-cert: DFN-CERT-2022-0365

High (CVSS: 9.8)
NVT: PHP 'var_unserializer' Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.3.10
Fixed version: 5.6.26

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

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

Affected Software/OS
PHP versions prior to 5.6.26 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'var_unserializer' Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.809322
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-7411
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/93009
cert-bund: CB-K16/1958
cert-bund: CB-K16/1543
cert-bund: CB-K16/1532
cert-bund: CB-K16/1426
dfn-cert: DFN-CERT-2016-2063
dfn-cert: DFN-CERT-2016-1639
dfn-cert: DFN-CERT-2016-1631
dfn-cert: DFN-CERT-2016-1495

High (CVSS: 9.8)
NVT: WordPress Multiple Vulnerabilities (Dec 2018) - Windows

Summary

... continues on next page ...

... continued from previous page ...

WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.6.1
Fixed version:     4.6.13
Installation
path / port:       /wordpress
```

Solution:
Solution type: VendorFix
The issues have been fixed in version 5.0.1. Updated versions of WordPress 4.9 and older releases are also available.
Please see the references for more information.

Affected Software/OS
All versions since WordPress 3.7 up to 5.0.

Vulnerability Insight
The following vulnerabilities exist:
- Authors could alter meta data to delete files that they weren't authorized to.
- Authors could create posts of unauthorized post types with specially crafted input.
- Contributors could craft meta data in a way that resulted in PHP object injection.
- Contributors could edit new comments from higher-privileged users, potentially leading to a cross-site scripting vulnerability.
- Specially crafted URL inputs could lead to a cross-site scripting vulnerability in some circumstances. WordPress itself was not affected, but plugins could be in some situations.
- The user activation screen could be indexed by search engines in some uncommon configurations, leading to exposure of email addresses, and in some rare cases, default generated passwords.
- Authors on Apache-hosted sites could upload specifically crafted files that bypass MIME verification, leading to a cross-site scripting vulnerability.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (Dec 2018) - Windows`
OID:1.3.6.1.4.1.25623.1.0.112465
Version used: `2023-03-01T10:20:05Z`

References

```
cve: CVE-2018-20147
cve: CVE-2018-20148
cve: CVE-2018-20149
cve: CVE-2018-20150
cve: CVE-2018-20151
cve: CVE-2018-20152
cve: CVE-2018-20153
url: https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
```

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/106220
cert-bund: CB-K18/1174
dfn-cert: DFN-CERT-2018-2545

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

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 Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808674
Version used: 2022-04-13T13:17:10Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-4644
cve: CVE-2015-4643
cve: CVE-2015-4598
cve: CVE-2015-4642
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/75291
url: http://www.securityfocus.com/bid/75292
url: http://www.securityfocus.com/bid/75244
url: http://www.securityfocus.com/bid/75290
cert-bund: CB-K16/0944
cert-bund: CB-K15/1261
cert-bund: CB-K15/1158
cert-bund: CB-K15/1031
cert-bund: CB-K15/0973
cert-bund: CB-K15/0966
cert-bund: CB-K15/0942
cert-bund: CB-K15/0936
cert-bund: CB-K15/0880
cert-bund: CB-K15/0854
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2015-1335
dfn-cert: DFN-CERT-2015-1217
dfn-cert: DFN-CERT-2015-1083
dfn-cert: DFN-CERT-2015-1021
dfn-cert: DFN-CERT-2015-1017
dfn-cert: DFN-CERT-2015-0989
dfn-cert: DFN-CERT-2015-0983
dfn-cert: DFN-CERT-2015-0926
dfn-cert: DFN-CERT-2015-0900

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 04 - Jul16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.4.44

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

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

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

Vulnerability Insight
Multiple flaws exist 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 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808605
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-8867
cve: CVE-2015-8876
cve: CVE-2015-8873
cve: CVE-2015-8835
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/87481
url: http://www.securityfocus.com/bid/90867
url: http://www.securityfocus.com/bid/84426
url: http://www.securityfocus.com/bid/90712
cert-bund: CB-K17/0318

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1776
cert-bund: CB-K16/1190
cert-bund: CB-K16/1179
cert-bund: CB-K16/0944
cert-bund: CB-K16/0937
cert-bund: CB-K16/0912
cert-bund: CB-K16/0911
cert-bund: CB-K16/0868
cert-bund: CB-K16/0705
cert-bund: CB-K16/0623
cert-bund: CB-K16/0614
dfn-cert: DFN-CERT-2017-0325
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1265
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0996
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0944
dfn-cert: DFN-CERT-2016-0924
dfn-cert: DFN-CERT-2016-0764
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0659
```

High (CVSS: 9.8)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.6.7`

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

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions prior to 5.6.7 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'type confusion' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808672
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2015-4601`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/75246`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K15/1158`
`cert-bund: CB-K15/1031`
`cert-bund: CB-K15/0966`
`cert-bund: CB-K15/0942`
`cert-bund: CB-K15/0936`
`cert-bund: CB-K15/0854`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2015-1217`
`dfn-cert: DFN-CERT-2015-1083`
`dfn-cert: DFN-CERT-2015-1017`
`dfn-cert: DFN-CERT-2015-0989`
`dfn-cert: DFN-CERT-2015-0983`
`dfn-cert: DFN-CERT-2015-0900`

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities - 03 - Sep16 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to PHP version 5.6.26, or 7.0.11, or later.

Affected Software/OS
PHP versions prior to 5.6.26 and 7.x before 7.0.11 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 03 - Sep16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809316
Version used: `2023-03-24T10:19:42Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-7412`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-7413
cve: CVE-2016-7414
cve: CVE-2016-7416
cve: CVE-2016-7417
cve: CVE-2016-7418
url: http://www.php.net/ChangeLog-7.php
url: http://www.securityfocus.com/bid/93005
url: http://www.securityfocus.com/bid/93006
url: http://www.securityfocus.com/bid/93004
url: http://www.securityfocus.com/bid/93022
url: http://www.securityfocus.com/bid/93008
url: http://www.securityfocus.com/bid/93007
url: http://www.securityfocus.com/bid/93011
url: http://www.php.net/ChangeLog-5.php
cert-bund: CB-K16/1958
cert-bund: CB-K16/1549
cert-bund: CB-K16/1543
cert-bund: CB-K16/1532
cert-bund: CB-K16/1426
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2016-2063
dfn-cert: DFN-CERT-2016-1641
dfn-cert: DFN-CERT-2016-1639
dfn-cert: DFN-CERT-2016-1631
dfn-cert: DFN-CERT-2016-1495
```

High (CVSS: 9.8)
NVT: PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.29
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.29, 7.0.14 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions prior to 5.6.29 and 7.0.x prior to 7.0.14.

Vulnerability Insight
The php_wddx_push_element function in ext/wddx/wddx.c allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.117804
Version used: `2021-11-29T14:44:44Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-9935`
`url: https://www.php.net/ChangeLog-7.php#7.0.14`
`url: https://www.php.net/ChangeLog-5.php#5.6.29`
`url: https://bugs.php.net/bug.php?id=73631`
`cert-bund: CB-K17/0527`
`cert-bund: CB-K17/0327`
`cert-bund: CB-K17/0269`
`cert-bund: CB-K17/0053`
`cert-bund: CB-K17/0015`
`cert-bund: CB-K16/2015`
`cert-bund: CB-K16/1982`
`dfn-cert: DFN-CERT-2018-0835`
`dfn-cert: DFN-CERT-2017-0532`
`dfn-cert: DFN-CERT-2017-0334`
`dfn-cert: DFN-CERT-2017-0274`
`dfn-cert: DFN-CERT-2017-0058`
`dfn-cert: DFN-CERT-2017-0016`
`dfn-cert: DFN-CERT-2016-2130`
`dfn-cert: DFN-CERT-2016-2084`

High (CVSS: 9.8)
NVT: WordPress Multiple Vulnerabilities - Oct19 (Windows)

Summary

... continues on next page ...

... continued from previous page ...

WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.16
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.31, 3.8.31, 3.9.29, 4.0.28, 4.1.28, 4.2.25, 4.3.21, 4.4.20, 4.5.19, 4.6.16, 4.7.15, 4.8.11, 4.9.12, 5.0.7, 5.1.3, 5.2.4 or later.

Affected Software/OS
WordPress version 5.2.3 and earlier.

Vulnerability Insight
WordPress is prone to multiple vulnerabilities:
- Stored XSS via the Customizer
- Possibility to view unauthenticated posts
- Stored XSS to inject Javascript into style tags
- Cache poisoning of JSON GET requests via the Vary: Origin header
- Server-Side Request Forgery in URL validation
- Issues in referrer validation in the admin

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities - Oct19 (Windows)
OID:1.3.6.1.4.1.25623.1.0.143061
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2019-17669
cve: CVE-2019-17670
cve: CVE-2019-17671
cve: CVE-2019-17672
cve: CVE-2019-17673
cve: CVE-2019-17674
cve: CVE-2019-17675
url: https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
cert-bund: WID-SEC-2022-1658
cert-bund: CB-K19/0903
dfn-cert: DFN-CERT-2022-2231
dfn-cert: DFN-CERT-2020-1991
dfn-cert: DFN-CERT-2020-0955
dfn-cert: DFN-CERT-2020-0030

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-2297

High (CVSS: 9.8)
NVT: WordPress < 5.8 Missing 'Update URI' Plugin Header Vulnerability - Windows

Summary
WordPress is prone to a missing 'Update URI' plugin header vulnerability.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 5.8
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 5.8 or later.

Affected Software/OS
WordPress prior to version 5.8.

Vulnerability Insight
WordPress lacks support for the Update URI plugin header. This makes it easier for remote attackers to execute arbitrary code via a supply-chain attack against WordPress installations that use any plugin for which the slug satisfies the naming constraints of the WordPress.org Plugin Directory but is not yet present in that directory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress < 5.8 Missing 'Update URI' Plugin Header Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.147225
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2021-44223
url: https://make.wordpress.org/core/2021/06/29/introducing-update-uri-plugin-he
↪ader-in-wordpress-5-8/
url: https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-yo
↪u-pwned/
cert-bund: CB-K21/1242

High (CVSS: 9.8)
NVT: WordPress Multiple Vulnerabilities - Dec19 (Windows)

... continues on next page ...

... continued from previous page ...

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.17
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.31, 3.8.31, 3.9.29, 4.0.28, 4.1.28, 4.2.25, 4.3.21, 4.4.20, 4.5.19, 4.6.16, 4.7.15, 4.8.11, 4.9.12, 5.0.7, 5.1.3, 5.2.4 or later.

Affected Software/OS
WordPress version 5.3.1 and earlier.

Vulnerability Insight
The following vulnerabilities exist:
- An issue where an unprivileged user could make a post sticky via the REST API
- The function wp_targeted_link_rel() can be used in a particular way to result in a stored cross-site scripting (XSS) vulnerability
- An issue where cross-site scripting (XSS) could be stored in well-crafted links
- wp_kses_bad_protocol() is not aware of the named colon attribute
- A stored XSS vulnerability using block editor content.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities - Dec19 (Windows)
OID:1.3.6.1.4.1.25623.1.0.112675
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2019-16773
cve: CVE-2019-16780
cve: CVE-2019-16781
cve: CVE-2019-16788
cve: CVE-2019-20041
cve: CVE-2019-20042
cve: CVE-2019-20043
url: https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance
↪-release/
cert-bund: CB-K20/0017
cert-bund: CB-K19/1078
dfn-cert: DFN-CERT-2020-0955
dfn-cert: DFN-CERT-2020-0075

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0030

High (CVSS: 9.8)
NVT: WordPress Multiple Vulnerabilities (May 2021) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.21
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.36, 3.8.36, 3.9.34, 4.0.33, 4.1.33, 4.2.30, 4.3.26, 4.4.25, 4.5.24, 4.6.21, 4.7.21, 4.8.17, 4.9.18, 5.0.13, 5.1.10, 5.2.11, 5.3.8, 5.4.6, 5.5.5, 5.6.4, 5.7.2 or later.

Affected Software/OS
WordPress versions 3.7 through 5.7.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2018-19296: PHPMailer is vulnerable to an object injection attack.
- CVE-2021-29450: PHPMailer allows object injection through Phar Deserialization via addAttachment with a UNC pathname.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities (May 2021) - Windows
OID:1.3.6.1.4.1.25623.1.0.145945
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2018-19296
cve: CVE-2020-36326
url: https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/
cert-bund: CB-K21/0527
dfn-cert: DFN-CERT-2021-1036
dfn-cert: DFN-CERT-2021-0932
dfn-cert: DFN-CERT-2018-2403
dfn-cert: DFN-CERT-2018-2357

High (CVSS: 9.8)
NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a stack buffer overflow vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Affected Software/OS
PHP versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Windows

Vulnerability Insight
Multiple flaws are due to
- Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script.
- Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807092
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2015-5590
cve: CVE-2015-8838
cve: CVE-2015-5589
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/75970
url: http://www.securityfocus.com/bid/88763
url: http://www.securityfocus.com/bid/75974
url: https://bugs.php.net/bug.php?id=69923
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0623
cert-bund: CB-K16/0614
cert-bund: CB-K16/0422
cert-bund: CB-K15/1439
cert-bund: CB-K15/1261
cert-bund: CB-K15/1147
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0659
dfn-cert: DFN-CERT-2016-0460
dfn-cert: DFN-CERT-2015-1515
dfn-cert: DFN-CERT-2015-1335
dfn-cert: DFN-CERT-2015-1203
```

High (CVSS: 9.8)
NVT: PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to a use-after-free vulnerability in a used third-pary library.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     7.1.32
Installation
path / port:       8585/tcp
```

Impact

This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to version 7.1.32, 7.3.9 or later.

Affected Software/OS
PHP version before 7.1.32 and 7.3.x before 7.3.9.

Vulnerability Insight
The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP.
The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe().

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108634
Version used: `2022-07-22T10:11:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2019-13224`
`url: http://bugs.php.net/78380`
`url: https://www.php.net/ChangeLog-7.php#7.3.9`
`url: https://www.php.net/ChangeLog-7.php#7.1.32`
`cert-bund: CB-K20/1030`
`dfn-cert: DFN-CERT-2022-2107`
`dfn-cert: DFN-CERT-2020-2412`
`dfn-cert: DFN-CERT-2020-2105`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2019-1804`
`dfn-cert: DFN-CERT-2019-1471`
`dfn-cert: DFN-CERT-2019-1424`

High (CVSS: 9.8)
NVT: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows

Product detection result
`cpe:/a:apache:http_server:2.2.21`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

... continues on next page ...

... continued from previous page ...

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.4.49
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.49 or later.

Affected Software/OS
Apache HTTP Server version 2.4.48 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-34798: NULL pointer dereference in httpd core
- CVE-2021-39275: ap_escape_quotes buffer overflow
- CVE-2021-40438: mod_proxy SSRF

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.146726
Version used: 2022-08-09T10:11:17Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2021-34798
cve: CVE-2021-39275
cve: CVE-2021-40438
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2022-1298
cert-bund: WID-SEC-2022-1189

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0724
cert-bund: WID-SEC-2022-0190
cert-bund: CB-K22/0476
cert-bund: CB-K22/0465
cert-bund: CB-K22/0463
cert-bund: CB-K21/0992
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-0904
dfn-cert: DFN-CERT-2022-0878
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0869
dfn-cert: DFN-CERT-2022-0672
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2021-2629
dfn-cert: DFN-CERT-2021-2471
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2164
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-2098
dfn-cert: DFN-CERT-2021-2090
dfn-cert: DFN-CERT-2021-2047
dfn-cert: DFN-CERT-2021-2020
dfn-cert: DFN-CERT-2021-1961
```

High (CVSS: 9.8)
NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to a stack buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     5.6.34
Installation
path / port:       8585/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812820
Version used: `2022-04-13T07:21:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-7584`
`url: http://php.net/ChangeLog-7.php`
`url: http://www.securityfocus.com/bid/103204`
`url: https://bugs.php.net/bug.php?id=75981`
`cert-bund: CB-K18/0698`
`cert-bund: CB-K18/0498`
`cert-bund: CB-K18/0383`
`dfn-cert: DFN-CERT-2020-0680`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2018-1232`
`dfn-cert: DFN-CERT-2018-1059`
`dfn-cert: DFN-CERT-2018-0733`
`dfn-cert: DFN-CERT-2018-0576`
`dfn-cert: DFN-CERT-2018-0537`
`dfn-cert: DFN-CERT-2018-0399`

High (CVSS: 9.8)
NVT: WordPress 'esc_sql' Function SQL Injection Vulnerability - Nov 2017 (Windows)

Summary
WordPress is prone to an SQL injection vulnerability.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.8.3`

Impact
Successful exploitation will allow remote attackers to execute arbitrary commands.

Solution:
Solution type: VendorFix
Update to WordPress version 4.8.3 or later.

Affected Software/OS
WordPress versions 4.8.2 and earlier

Vulnerability Insight
The flaw exists because '$wpdb->prepare' function can create unexpected and unsafe queries.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress 'esc_sql' Function SQL Injection Vulnerability - Nov 2017 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811887
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2017-16510`
`url: https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release`
`cert-bund: CB-K18/0122`
`dfn-cert: DFN-CERT-2018-0126`

High (CVSS: 9.8)
NVT: WordPress Ninja Forms Plugin < 3.3.21.2 SQLi Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
`Installed version: 2.9.42`
`Fixed version: 3.3.21.2`
`Installation`
`path / port: /wordpress/wp-content/plugins/ninja-forms`

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 3.3.21.2 or later.

Affected Software/OS
WordPress Ninja Forms plugin before version 3.3.21.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.3.21.2 SQLi Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112631
Version used: `2023-01-17T10:10:58Z`

References
`cve: CVE-2019-15025`
`url: https://wordpress.org/plugins/ninja-forms/#developers`

High (CVSS: 9.8)
NVT: WordPress < 4.7.2 Multiple Security Vulnerabilities (Windows)

Summary
WordPress is prone to multiple security vulnerabilities because it fails to sanitize user-supplied input.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.7.2`

Impact
Successfully exploiting this issue allow remote attacker to e.g. obtain sensitive information or inject arbitrary web script or HTML.

Solution:
Solution type: VendorFix
Update to WordPress version 4.7.2.

Affected Software/OS
WordPress versions 4.7.1 and earlier.

Vulnerability Insight
Multiple flaws are due to:
- The user interface for assigning taxonomy terms in Press This is shown to users who do not have permissions to use it.

... continues on next page ...

... continued from previous page ...

- P_Query is vulnerable to a SQL injection (SQLi) when passing unsafe data. WordPress core is not directly vulnerable to this issue, but hardening was added to prevent plugins and themes from accidentally causing a vulnerability.
- A cross-site scripting (XSS) vulnerability was discovered in the posts list table.
- An unauthenticated privilege escalation vulnerability was discovered in a REST API endpoint.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 4.7.2 Multiple Security Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108069
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2017-5610`
`cve: CVE-2017-5611`
`cve: CVE-2017-5612`
`cve: CVE-2017-1001000`
`url: https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-securit`
`↪y-fix-in-wordpress-4-7-2/`
`url: https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/`
`url: https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-r`
`↪est-api.html`
`url: http://www.secpod.com/blog/wordpress-rest-api-zero-day-privilege-escalation`
`↪-vulnerability`
`cert-bund: CB-K17/0154`
`dfn-cert: DFN-CERT-2017-0193`
`dfn-cert: DFN-CERT-2017-0159`

High (CVSS: 9.8)
NVT: WordPress < 4.8.2 Multiple Vulnerabilities - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.8.2`
`Installation`
`path / port: /wordpress`

Impact
Successful exploitation will allow remote attackers to conduct XSS, SQLi, directory traversal and open redirect attacks.

Solution:
Solution type: VendorFix
Update to version 4.8.2 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress versions 4.8.1 and earlier.

Vulnerability Insight
The following flaws exist:
- CVE-2017-14718: A cross-site scripting (XSS) vulnerability was discovered in the link modal.
- CVE-2017-14719: A path traversal vulnerability was discovered in the file unzipping code.
- CVE-2017-14720: A cross-site scripting (XSS) vulnerability was discovered in template names.
- CVE-2017-14721: A cross-site scripting (XSS) vulnerability was discovered in the plugin editor.
- CVE-2017-14722: A path traversal vulnerability was discovered in the customizer.
- CVE-2017-14723: $wpdb->prepare() can create unexpected and unsafe queries leading to potential SQL injection (SQLi). WordPress core is not directly vulnerable to this issue, but hardening was added to prevent plugins and themes from accidentally causing a vulnerability.
- CVE-2017-14724: A cross-site scripting (XSS) vulnerability was discovered in the oEmbed discovery.
- CVE-2017-14725: An open redirect was discovered on the user and term edit screens.
- CVE-2017-14726: A cross-site scripting (XSS) vulnerability was discovered in the visual editor.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 4.8.2 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.811783
Version used: `2023-03-01T10:20:05Z`

References
```
cve: CVE-2017-14718
cve: CVE-2017-14719
cve: CVE-2017-14720
cve: CVE-2017-14721
cve: CVE-2017-14722
cve: CVE-2017-14723
cve: CVE-2017-14724
cve: CVE-2017-14725
cve: CVE-2017-14726
url: https://wordpress.org/documentation/wordpress-version/version-4-8-2/
url: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance
↪-release/
cert-bund: CB-K17/1722
dfn-cert: DFN-CERT-2017-1802
```

High (CVSS: 9.8)
NVT: WordPress Multiple Vulnerabilities - Oct20 (Windows)

Summary

... continues on next page ...

... continued from previous page ...

WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.20
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.35, 3.8.35, 3.9.33, 4.0.32, 4.1.32, 4.2.29, 4.3.25, 4.4.24, 4.5.23, 4.6.20, 4.7.19, 4.8.15, 4.9.16, 5.0.11, 5.1.7, 5.2.8, 5.3.5, 5.4.3, 5.5.2 or later.

Affected Software/OS
All supported WordPress versions 3.7 - 5.5.1. Older versions might be affected as well.

Vulnerability Insight
The following vulnerabilities exist:
- Multiple cross-site scripting
- Insecure Deserialization
- Privilege escalation in XML-RPC
- DoS attack which could lead to a remote code execution
- Arbitrary file deletion
- Cross request forgery (CSRF)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities - Oct20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.144873
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2020-28040
cve: CVE-2020-28039
cve: CVE-2020-28038
cve: CVE-2020-28037
cve: CVE-2020-28036
cve: CVE-2020-28035
cve: CVE-2020-28034
cve: CVE-2020-28033
cve: CVE-2020-28032
url: https://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance
↪-release/
cert-bund: CB-K20/1058
dfn-cert: DFN-CERT-2020-2360

High (CVSS: 9.6)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to XML entity expansion and XML external entity vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.22, or 5.6.6, or later.

Affected Software/OS
PHP versions prior to 5.5.22 and 5.6.x before 5.6.6 on Windows

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.808614
Version used: 2022-07-22T10:11:18Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-8866
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/87470
cert-bund: CB-K18/0028

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1776
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0705
cert-bund: CB-K16/0614
dfn-cert: DFN-CERT-2018-0010
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0764
dfn-cert: DFN-CERT-2016-0659

High (CVSS: 9.1)
NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Windows

Vulnerability Insight
The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Windows)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.807089
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-1903
url: https://bugs.php.net/bug.php?id=70976
url: http://www.securityfocus.com/bid/79916
url: http://www.openwall.com/lists/oss-security/2016/01/14/8
cert-bund: CB-K16/1776
cert-bund: CB-K16/0614
cert-bund: CB-K16/0161
cert-bund: CB-K16/0136
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-0659
dfn-cert: DFN-CERT-2016-0176
dfn-cert: DFN-CERT-2016-0154

High (CVSS: 9.1)
NVT: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.2.34
Installation
path / port: 8585/tcp

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

... continues on next page ...

... continued from previous page ...

Update 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.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811236
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.21`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2017-9788`
`url: http://www.securitytracker.com/id/1038906`
`url: http://www.securityfocus.com/bid/99569`
`url: http://httpd.apache.org/security/vulnerabilities_22.html`
`url: http://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K18/0066`
`cert-bund: CB-K17/2013`
`cert-bund: CB-K17/1980`
`cert-bund: CB-K17/1936`
`cert-bund: CB-K17/1871`
`cert-bund: CB-K17/1854`
`cert-bund: CB-K17/1842`
`cert-bund: CB-K17/1768`
`cert-bund: CB-K17/1747`
`cert-bund: CB-K17/1622`
`cert-bund: CB-K17/1558`
`cert-bund: CB-K17/1382`
`cert-bund: CB-K17/1197`
`cert-bund: CB-K17/1177`
`cert-bund: CB-K17/1023`
`dfn-cert: DFN-CERT-2019-0358`
`dfn-cert: DFN-CERT-2018-0077`
`dfn-cert: DFN-CERT-2017-2104`
`dfn-cert: DFN-CERT-2017-2070`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1843
dfn-cert: DFN-CERT-2017-1828
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1240
dfn-cert: DFN-CERT-2017-1217
dfn-cert: DFN-CERT-2017-1058
```

High (CVSS: 9.1)
NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
```
Installed version: 5.3.10
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
Update to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Windows.

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

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

... continues on next page ...

... continued from previous page ...

Details: PHP Denial of Service Vulnerability - 02 - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.809138
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-5114
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/81808
cert-bund: CB-K16/1776
cert-bund: CB-K16/1179
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0911
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0944

High (CVSS: 9.1)
NVT: PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.27
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.27, 7.3.14, 7.4.2 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions before 7.2.27, 7.3.x and 7.4.x.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- OOB read in php_strip_tags_ex (CVE-2020-7059)
- Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143393
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2020-7059`
`cve: CVE-2020-7060`
`url: https://www.php.net/ChangeLog-7.php#7.2.27`
`url: https://www.php.net/ChangeLog-7.php#7.3.14`
`url: https://www.php.net/ChangeLog-7.php#7.4.2`
`cert-bund: WID-SEC-2022-2121`
`cert-bund: CB-K20/1199`
`cert-bund: CB-K20/0067`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-0485`
`dfn-cert: DFN-CERT-2020-0422`
`dfn-cert: DFN-CERT-2020-0415`
`dfn-cert: DFN-CERT-2020-0382`
`dfn-cert: DFN-CERT-2020-0342`
`dfn-cert: DFN-CERT-2020-0339`
`dfn-cert: DFN-CERT-2020-0337`
`dfn-cert: DFN-CERT-2020-0139`

High (CVSS: 8.8)
NVT: WordPress < 4.7.1 Multiple Security Vulnerabilities (Windows)

Summary

... continues on next page ...

... continued from previous page ...

WordPress is prone to multiple security vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.7.1`

Impact
Successfully exploiting this issue allow remote attacker to e.g. obtain sensitive information or inject arbitrary web script or HTML.

Solution:
Solution type: VendorFix
Update to WordPress version 4.7.1.

Affected Software/OS
WordPress versions 4.7 and earlier on Windows.

Vulnerability Insight
Multiple flaws are due to:
- Cross-site scripting (XSS) via the plugin name or version header on update-core.php
- Cross-site request forgery (CSRF) bypass via uploading a Flash file
- Cross-site scripting (XSS) via theme name fallback
- Post via email checks mail.example.com if default settings are not changed
- Cross-site request forgery (CSRF) in the accessibility mode of widget editing
- Weak cryptographic security for multisite activation key

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 4.7.1 Multiple Security Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108047
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2017-5493`
`cve: CVE-2017-5492`
`cve: CVE-2017-5491`
`cve: CVE-2017-5490`
`cve: CVE-2017-5489`
`cve: CVE-2017-5488`
`cve: CVE-2017-5487`
`cve: CVE-2016-10066`
`url: https://wpvulndb.com/wordpresses/47`
`url: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance`
`↪-release/`
`cert-bund: CB-K17/0060`
`dfn-cert: DFN-CERT-2017-0193`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-0056

High (CVSS: 8.8)
NVT: WordPress RCE Vulnerability CVE-2019-8942 (Windows)

Summary
WordPress allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.9.9
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 4.9.9, 5.0.1 or later.

Affected Software/OS
WordPress prior version 4.9.9 and 5.0.1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress RCE Vulnerability CVE-2019-8942 (Windows)
OID:1.3.6.1.4.1.25623.1.0.142030
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2019-8942
url: https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
url: http://www.securityfocus.com/bid/107088
cert-bund: CB-K19/0155
dfn-cert: DFN-CERT-2019-0642
dfn-cert: DFN-CERT-2018-2545

High (CVSS: 8.8)
NVT: WordPress < 4.7.5 Multiple Security Vulnerabilities (Win)

Summary
WordPress is prone to the following security vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.7.5

Impact
An attacker may leverage these issues to execute HTML and script code in the browser of an unsuspecting user in the context of the affected site, perform certain unauthorized actions actions, or bypass certain security restrictions.

Solution:
Solution type: VendorFix
Update to 4.7.5.

Affected Software/OS
WordPress prior to 4.7.5 versions are vulnerable

Vulnerability Insight
WordPress is prone to the following security vulnerabilities:
1. An open-redirect vulnerability
2. Multiple security-bypass vulnerabilities
3. Multiple cross-site scripting vulnerabilities
4. A cross-site request-forgery vulnerability

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress < 4.7.5 Multiple Security Vulnerabilities (Win)
OID:1.3.6.1.4.1.25623.1.0.107200
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2017-9061
cve: CVE-2017-9062
cve: CVE-2017-9063
cve: CVE-2017-9064
cve: CVE-2017-9065
cve: CVE-2017-9066
url: http://www.securityfocus.com/bid/98509
cert-bund: CB-K18/0122
cert-bund: CB-K17/0831
dfn-cert: DFN-CERT-2018-0126
dfn-cert: DFN-CERT-2017-0859

High (CVSS: 8.8)
NVT: WampServer < 3.1.3 CSRF Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

WampServer is prone to a cross site request forgery (CSRF) vulnerability.

Vulnerability Detection Result
Installed version: 2.2
Fixed version: 3.1.3

Solution:
Solution type: VendorFix
Update to version 3.1.3 or later.

Affected Software/OS
WampServer 3.1.2 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WampServer < 3.1.3 CSRF Vulnerability
OID:1.3.6.1.4.1.25623.1.0.140891
Version used: 2022-05-31T13:29:50Z

References
cve: CVE-2018-8817
url: http://forum.wampserver.com/read.php?2%2C138295%2C150722%2Cpage%3D6%23msg-1
↪50722

High (CVSS: 8.8)
NVT: WordPress Multiple Vulnerabilities - March19 (Windows)

Summary
WordPress is prone to a Cross Site Request Forgery (CSRF) vulnerability in a comment form which leads to HTML injection and cross-site scripting (XSS) attacks.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.14
Installation
path / port: /wordpress

Impact
Chaining all found vulnerabilities, an attacker might be able to execute remote code on the affected system, getting access to the underlying hosting system.

Solution:
Solution type: VendorFix
Update to 5.1.1, 5.0.4, 4.9.10, 4.8.9, 4.7.13, 4.6.14, 4.5.17, 4.4.18, 4.3.19, 4.2.23, 4.1.26, 4.0.26, 3.9.27 or any later version.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress 5.1.x prior to 5.1.1, 5.0.x prior to 5.0.4, 4.9.x prior to 4.9.10, 4.8.x prior to 4.8.9, 4.7.x prior to 4.7.13, 4.6.x prior to 4.6.14, 4.5.x prior to 4.5.17, 4.4.x prior to 4.4.18, 4.3.x prior to 4.3.19, 4.2.x prior to 4.2.23, 4.1.x prior to 4.1.26, 4.0.x prior to 4.0.26 and 3.9.x prior to 3.9.27.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities - March19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108559
Version used: `2023-03-01T10:20:05Z`

References
```
cve: CVE-2019-9787
url: https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
url: https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403
↪654fe4d080b
url: https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance
↪-release/
url: https://wordpress.org/support/wordpress-version/version-5-1-1/
cert-bund: CB-K19/0228
dfn-cert: DFN-CERT-2020-0955
dfn-cert: DFN-CERT-2019-0642
dfn-cert: DFN-CERT-2019-0517
```

High (CVSS: 8.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Windows)

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP is prone to denial of service and unspecified vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
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:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to PHP version 5.6.18, or 7.0.3, or later.

Affected Software/OS
PHP versions prior to 5.6.18 and 7.x before 7.0.3 on Windows

Vulnerability Insight
The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808608
Version used: `2022-07-22T10:11:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-4343`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/89179`
`url: http://www.openwall.com/lists/oss-security/2016/04/28/2`
`cert-bund: CB-K16/1776`
`cert-bund: CB-K16/0796`
`cert-bund: CB-K16/0779`
`cert-bund: CB-K16/0760`
`dfn-cert: DFN-CERT-2016-1882`
`dfn-cert: DFN-CERT-2016-0847`
`dfn-cert: DFN-CERT-2016-0835`
`dfn-cert: DFN-CERT-2016-0814`

High (CVSS: 8.8)
NVT: WordPress Multiple Vulnerabilities (Mar 2022) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     4.6.23
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.38, 3.8.38, 3.9.36, 4.0.35, 4.1.35, 4.2.32, 4.3.28, 4.4.27, 4.5.26, 4.6.23, 4.7.23, 4.8.19, 4.9.20, 5.0.16, 5.1.13, 5.2.15, 5.3.12, 5.4.10, 5.5.9, 5.6.8, 5.7.6, 5.8.4, 5.9.2 or later.

Affected Software/OS
WordPress version 5.9.1 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- No CVE: Prototype pollution via the Gutenberg wordpress/url package
- CVE-2021-20083: Prototype pollution in a jQuery dependency
- No CVE: Stored cross-site scripting (XSS), only affecting version 5.9.0 and 5.9.1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities (Mar 2022) - Windows
OID:1.3.6.1.4.1.25623.1.0.147790
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2021-20083
url: https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-rel
↪ease/
url: https://www.wordfence.com/blog/2022/03/wordpress-5-9-2-security-update-fixe
↪s-xss-and-prototype-pollution-vulnerabilities/
url: https://packetstormsecurity.com/files/166299/WordPress-Core-5.9.0-5.9.1-Cro
↪ss-Site-Scripting.html
cert-bund: CB-K22/0314
dfn-cert: DFN-CERT-2022-0571

High (CVSS: 8.8)
NVT: WordPress Arbitrary File Deletion Vulnerability (Jun 2018) - Windows

Summary
WordPress is prone to an arbitrary file deletion vulnerability.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.9.7
Installation
path / port: /wordpress

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to delete any file of the wordPress installation and any other file on the server on which the PHP process user has the proper permissions to delete. Also capability of arbitrary file deletion can be used to circumvent some security measures and execute arbitrary code on the webserver.

Solution:
Solution type: VendorFix
Update to version 4.9.7.

Affected Software/OS
All wordPress versions through version 4.9.6.

Vulnerability Insight
The flaw exists due to an insufficient sanitization of user input data in the 'wp-includes/post.php' script before passing on to a file deletion function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Arbitrary File Deletion Vulnerability (Jun 2018) - Windows`
OID:1.3.6.1.4.1.25623.1.0.813454
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2018-12895`
`url: https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution`
`url: https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance`
`↪-release/`
`dfn-cert: DFN-CERT-2018-1483`
`dfn-cert: DFN-CERT-2018-1314`

High (CVSS: 8.8)
NVT: PHP Multiple Vulnerabilities May18 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version:     5.6.36`

... continues on next page ...

... continued from previous page ...

Installation
path / port: 8585/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
Update 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 Windows.

Vulnerability Insight
Multiple flaws exist due to
- An out of bounds read error in 'exif_read_data' function while processing crafted JPG data.
- An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence.
- An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP.
- An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities May18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.813159
Version used: 2021-06-03T02:00:18Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-10549
cve: CVE-2018-10546
cve: CVE-2018-10548
cve: CVE-2018-10547
url: http://www.php.net/ChangeLog-5.php#5.6.36

... continues on next page ...

... continued from previous page ...

```
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
cert-bund: CB-K18/0633
dfn-cert: DFN-CERT-2020-0680
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-1232
dfn-cert: DFN-CERT-2018-0920
dfn-cert: DFN-CERT-2018-0877
```

High (CVSS: 8.8)
NVT: WordPress < 4.9.1 Multiple Vulnerabilities (Windows)

Summary
WordPress prior to 4.9.1 is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     4.9.1
```

Impact
An attacker may leverage these issues to bypass access restrictions or conduct XSS via specific vectors.

Solution:
Solution type: VendorFix
Update to WordPress 4.9.1 or later.

Affected Software/OS
WordPress prior to version 4.9.1.

Vulnerability Insight
WordPress before 4.9.1 is prone to the following security vulnerabilities:
- wp-admin/user-new.php sets the newbloguser key to a string that can be directly derived from the user ID, which allows remote attackers to bypass intended access restrictions by entering this string. (CVE-2017-17091)
- wp-includes/functions.php does not require the unfiltered_html capability for upload of .js files, which might allow remote attackers to conduct XSS attacks via a crafted file. (CVE-2017-17092)
- wp-includes/general-template.php does not properly restrict the lang attribute of an HTML element, which might allow attackers to conduct XSS attacks via the language setting of a site. (CVE-2017-17093)
- wp-includes/feed.php does not properly restrict enclosures in RSS and Atom fields, which might allow attackers to conduct XSS attacks via a crafted URL. (CVE-2017-17094)

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

... continues on next page ...

... continued from previous page ...

Details: WordPress < 4.9.1 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.112147
Version used: 2023-07-14T16:09:27Z

References
cve: CVE-2017-17091
cve: CVE-2017-17092
cve: CVE-2017-17093
cve: CVE-2017-17094
url: https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance
↪-release/
url: https://codex.wordpress.org/Version_4.9.1
cert-bund: CB-K18/0122
dfn-cert: DFN-CERT-2018-0126

High (CVSS: 8.6)
NVT: PHP Multiple Vulnerabilities - 04 - Aug16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

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

Vulnerability Insight
Multiple flaws are due to:
- The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character.

... continues on next page ...

... continued from previous page ...

- The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - 04 - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808793
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2013-7456
cve: CVE-2016-5093
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/90946
url: http://www.securityfocus.com/bid/90859
url: http://www.php.net/ChangeLog-7.php
cert-bund: CB-K16/1776
cert-bund: CB-K16/1179
cert-bund: CB-K16/1045
cert-bund: CB-K16/0944
cert-bund: CB-K16/0937
cert-bund: CB-K16/0912
cert-bund: CB-K16/0911
cert-bund: CB-K16/0909
cert-bund: CB-K16/0801
cert-bund: CB-K16/0796
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1110
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0996
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0960
dfn-cert: DFN-CERT-2016-0944
dfn-cert: DFN-CERT-2016-0857
dfn-cert: DFN-CERT-2016-0847

High (CVSS: 8.6)
NVT: PHP Multiple Vulnerabilities - 03 - Aug16 (Windows)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.36, or 5.6.22, or later.

Affected Software/OS
PHP versions prior to 5.5.36 and 5.6.x before 5.6.22 on Windows

Vulnerability Insight
Multiple flaws are due to:
- An integer overflow in the fread function in 'ext/standard/file.c' script.
- An integer overflow in the php_html_entities function in 'ext/standard/html.c' script.
- An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - 03 - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808791
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-5096
cve: CVE-2016-5094
cve: CVE-2016-5095
url: http://www.php.net/ChangeLog-5.php

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/90861
url: http://www.securityfocus.com/bid/90857
url: http://www.securityfocus.com/bid/92144
cert-bund: CB-K16/1982
cert-bund: CB-K16/1776
cert-bund: CB-K16/1179
cert-bund: CB-K16/0944
cert-bund: CB-K16/0937
cert-bund: CB-K16/0912
cert-bund: CB-K16/0911
cert-bund: CB-K16/0909
cert-bund: CB-K16/0796
dfn-cert: DFN-CERT-2016-2084
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0996
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0960
dfn-cert: DFN-CERT-2016-0944
dfn-cert: DFN-CERT-2016-0847
```

High (CVSS: 8.1)
NVT: PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Windows

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP released new versions which include a security fix.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     7.4.30
Installation
path / port:       8585/tcp
```

Solution:

Solution type: VendorFix

Update to version 7.4.30, 8.0.20, 8.1.7 or later.

Affected Software/OS

PHP prior to version 7.4.30, 8.0.x through 8.0.19 and 8.1.x through 8.1.6.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-31625: Uninitialized array in pg_query_params()
- CVE-2022-31626: mysqlnd/pdo password buffer overflow

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Windows`
OID:1.3.6.1.4.1.25623.1.0.148250
Version used: `2022-09-30T10:11:44Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2022-31625`
`cve: CVE-2022-31626`
`url: https://www.php.net/ChangeLog-7.php#7.4.30`
`url: https://www.php.net/ChangeLog-8.php#8.0.20`
`url: https://www.php.net/ChangeLog-8.php#8.1.7`
`url: https://bugs.php.net/bug.php?id=81720`
`url: https://bugs.php.net/bug.php?id=81719`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2022-0255`
`cert-bund: CB-K22/0700`
`dfn-cert: DFN-CERT-2023-1600`
`dfn-cert: DFN-CERT-2022-2869`
`dfn-cert: DFN-CERT-2022-2639`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2022-2598`
`dfn-cert: DFN-CERT-2022-2500`
`dfn-cert: DFN-CERT-2022-2323`
`dfn-cert: DFN-CERT-2022-1881`
`dfn-cert: DFN-CERT-2022-1552`
`dfn-cert: DFN-CERT-2022-1516`
`dfn-cert: DFN-CERT-2022-1493`
`dfn-cert: DFN-CERT-2022-1473`
`dfn-cert: DFN-CERT-2022-1288`

High (CVSS: 8.1)
NVT: WordPress Multiple Vulnerabilities - May20 (Windows)

Summary

... continues on next page ...

... continued from previous page ...

WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.6.1
Fixed version:     4.6.18
Installation
path / port:       /wordpress
```

Solution:
Solution type: VendorFix
Update to version 3.7.33, 3.8.33, 3.9.31, 4.0.30, 4.1.30, 4.2.27, 4.3.23, 4.4.22, 4.5.21, 4.6.18, 4.7.17, 4.8.13, 4.9.14, 5.0.9, 5.1.5, 5.2.6, 5.3.3, 5.4.1 or later.

Affected Software/OS
WordPress versions 3.7 - 5.4.

Vulnerability Insight
WordPress is prone to multiple vulnerabilities:
- Specially crafted filenames in WordPress leading to XSS (CVE-2020-11026)
- Password reset links invalidation issue (CVE-2020-11027)
- Unauthenticated disclosure of certain private posts (CVE-2020-11028)
- Cross-site scripting in stats method (object cache) (CVE-2020-11029)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities - May20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.143817
Version used: `2023-03-01T10:20:05Z`

References

```
cve: CVE-2020-11026
cve: CVE-2020-11027
cve: CVE-2020-11028
cve: CVE-2020-11029
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-3gw
↪2-4656-pfr2
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7
↪v-jg8c-q6jw
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx
↪9-759f-6p2w
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-568
↪w-8m88-8g2c
cert-bund: CB-K20/0413
dfn-cert: DFN-CERT-2020-0990
dfn-cert: DFN-CERT-2020-0955
```

High (CVSS: 8.1)
NVT: WordPress Ninja Forms Plugin < 3.0.23 Multiple Vulnerabilities

Summary
The WordPress plugin 'Ninja Forms' is prone to a path traversal and unrestricted file upload vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.0.23
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.0.23 or later.

Affected Software/OS
WordPress Ninja Forms plugin prior to version 3.0.23

Vulnerability Insight
The plugin allows an attacker to traverse the file system to access files and execute code via the includes/fields/upload.php (aka upload/submit page) name and tmp_name parameters.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.0.23 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.124068
Version used: `2022-07-20T10:33:02Z`

References
```
url: https://www.onvio.nl/nieuws/ninjaforms-vulnerability
cve: CVE-2019-10869
url: https://wpvulndb.com/vulnerabilities/9272
```

High (CVSS: 8.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Windows)

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP is prone to a man-in-the-middle attack vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.3.10
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 Windows

Vulnerability Insight
The following flaws exist:
- The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables.
- 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications
- An unspecified flaw in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808627
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-5385
cve: CVE-2016-6128
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/91821
url: http://www.securityfocus.com/bid/91509
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

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1252
cert-bund: CB-K16/1941
cert-bund: CB-K16/1854
cert-bund: CB-K16/1776
cert-bund: CB-K16/1549
cert-bund: CB-K16/1499
cert-bund: CB-K16/1407
cert-bund: CB-K16/1283
cert-bund: CB-K16/1248
cert-bund: CB-K16/1179
cert-bund: CB-K16/1115
cert-bund: CB-K16/1110
cert-bund: CB-K16/1106
cert-bund: CB-K16/1092
cert-bund: CB-K16/1077
cert-bund: CB-K16/1045
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2016-2047
dfn-cert: DFN-CERT-2016-1961
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1641
dfn-cert: DFN-CERT-2016-1590
dfn-cert: DFN-CERT-2016-1498
dfn-cert: DFN-CERT-2016-1367
dfn-cert: DFN-CERT-2016-1326
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1184
dfn-cert: DFN-CERT-2016-1179
dfn-cert: DFN-CERT-2016-1178
dfn-cert: DFN-CERT-2016-1157
dfn-cert: DFN-CERT-2016-1144
dfn-cert: DFN-CERT-2016-1110
```

High (CVSS: 8.1)
NVT: Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

Apache HTTP Server is prone to a man-in-the-middle attack vulnerability.

Vulnerability Detection Result

```
Installed version: 2.2.21
```

... continues on next page ...

... continued from previous page ...

Fixed version: 2.4.24
Installation
path / port: 8585/tcp

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
Update to version 2.4.24, or 2.2.32, or later.

Affected Software/OS
Apache HTTP Server through 2.4.23.
NOTE: Apache HTTP Server 2.2.32 is not vulnerable.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808631
Version used: 2022-09-09T10:12:35Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2016-5387
url: https://www.apache.org/security/asf-httpoxy-response.txt
url: http://www.securityfocus.com/bid/91816
cert-bund: CB-K17/2013
cert-bund: CB-K17/1854
cert-bund: CB-K17/1842
cert-bund: CB-K17/1622
cert-bund: CB-K17/0527
cert-bund: CB-K17/0055
cert-bund: CB-K16/1995
cert-bund: CB-K16/1620
cert-bund: CB-K16/1289
cert-bund: CB-K16/1103

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1088
cert-bund: CB-K16/1087
dfn-cert: DFN-CERT-2017-2104
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-2108
dfn-cert: DFN-CERT-2016-1717
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1175
dfn-cert: DFN-CERT-2016-1162
dfn-cert: DFN-CERT-2016-1153
```

High (CVSS: 7.8)
NVT: PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a buffer overflow vulnerability.

Vulnerability Detection Result

`Installed version:`	`5.3.10`
`Fixed version:`	`8.0.22/8.1.9/8.2.0`
`Installation path / port:`	`8585/tcp`

Solution:
Solution type: VendorFix
Update to version 8.0.22, 8.1.9, 8.2.0 or later.

Affected Software/OS
PHP versions prior to 8.0.22 and 8.1.x prior to 8.1.9.

Vulnerability Insight
Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_WORKERS environment variable.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Windows`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.104645
Version used: 2023-03-24T10:19:42Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2022-4900
url: https://www.php.net/ChangeLog-8.php#8.2.0
url: https://www.php.net/ChangeLog-8.php#8.1.9
url: https://www.php.net/ChangeLog-8.php#8.0.22
url: https://github.com/php/php-src/issues/8989
url: https://github.com/php/php-src/pull/9000
url: https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d458
↪0d5
url: https://bugzilla.redhat.com/show_bug.cgi?id=2179880
cert-bund: WID-SEC-2023-0695
dfn-cert: DFN-CERT-2023-0681

High (CVSS: 7.8)
NVT: PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 8.0.28
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 8.0.28, 8.1.16, 8.2.3 or later.

Affected Software/OS
PHP versions prior to 8.0.28, 8.1.x prior to 8.1.16 and 8.2.x prior to 8.2.3.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following flaws exist:
- CVE-2023-0567: Fixed bug #81744 (Password_verify() always return true with some hash)
- CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolve code)
- CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Windows`
OID:1.3.6.1.4.1.25623.1.0.104542
Version used: `2023-02-16T10:19:47Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2023-0567`
`cve: CVE-2023-0568`
`cve: CVE-2023-0662`
`url: https://www.php.net/ChangeLog-8.php#8.2.3`
`url: https://www.php.net/ChangeLog-8.php#8.1.16`
`url: https://www.php.net/ChangeLog-8.php#8.0.28`
`url: https://www.php.net/archive/2023.php#2023-02-14-2`
`url: https://www.php.net/archive/2023.php#2023-02-14-3`
`url: https://www.php.net/archive/2023.php#2023-02-14-1`
`url: http://bugs.php.net/81744`
`url: http://bugs.php.net/81746`
`url: https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv`
`url: https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1022`
`cert-bund: WID-SEC-2023-0383`
`dfn-cert: DFN-CERT-2023-0994`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0462`
`dfn-cert: DFN-CERT-2023-0435`
`dfn-cert: DFN-CERT-2023-0336`

High (CVSS: 7.8)
NVT: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Windows

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an integer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 8.0.27
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 8.0.27, 8.1.14, 8.2.1 or later.

Affected Software/OS
PHP prior to version 8.0.27, version 8.1.x through 8.1.13 and 8.2.0.

Vulnerability Insight
Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Windows
OID:1.3.6.1.4.1.25623.1.0.149070
Version used: 2023-01-09T10:12:48Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2022-31631
url: https://www.php.net/ChangeLog-8.php#8.0.27
url: https://www.php.net/ChangeLog-8.php#8.1.14
url: https://www.php.net/ChangeLog-8.php#8.2.1
cert-bund: WID-SEC-2023-0035
dfn-cert: DFN-CERT-2023-0435
dfn-cert: DFN-CERT-2023-0422
dfn-cert: DFN-CERT-2023-0071
dfn-cert: DFN-CERT-2023-0034

High (CVSS: 7.5)
NVT: PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a privilege escalation vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.5.32
Installation
path / port: 8585/tcp

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

Solution:
Solution type: VendorFix
Update to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Affected Software/OS
PHP versions before 5.5.32, 7.0.x before 7.0.3, and 5.6.x before 5.6.18 on Windows.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.812513
Version used: 2023-01-19T10:10:48Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-10712

. . . continues on next page . . .

... continued from previous page ...

```
url: https://bugs.php.net/bug.php?id=71323
url: https://git.php.net/?p=php-src.git;a=commit;h=6297a117d77fa3a0df2e21ca926a9
↪2c231819cd5
cert-bund: CB-K18/0498
cert-bund: CB-K18/0350
dfn-cert: DFN-CERT-2019-1052
dfn-cert: DFN-CERT-2018-0576
dfn-cert: DFN-CERT-2018-0537
dfn-cert: DFN-CERT-2018-0380
```

High (CVSS: 7.5)
NVT: WordPress Multiple Vulnerabilities - May17 (Windows)

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.7.5`

Impact
Successfully exploiting will allow remote attacker to conduct cross site request forgery (CSRF) attacks, cross-site scripting (XSS) attacks and have other some unspecified impact.

Solution:
Solution type: VendorFix
Update to WordPress version 4.7.5 or later.

Affected Software/OS
WordPress versions 4.7.4 and prior on Windows.

Vulnerability Insight
Multiple flaws are due to:
- An insufficient redirect validation in the HTTP class.
- An improper handling of post meta data values in the XML-RPC API.
- The lack of capability checks for post meta data in the XML-RPC API.
- A cross site request forgery (CSRF) vulnerability in the filesystem credentials dialog.
- A cross-site scripting (XSS) vulnerability when attempting to upload very large files.
- A cross-site scripting (XSS) vulnerability related to the Customizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities - May17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811045
Version used: `2023-03-01T10:20:05Z`

... continues on next page ...

... continued from previous page ...

References
url: https://wordpress.org/news/2017/05/wordpress-4-7-5

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Mar13 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.23/5.4.13

Impact
Successful exploitation allows attackers to read arbitrary files and write wsdl files within the context of the affected application.

Solution:
Solution type: VendorFix
Update to PHP 5.4.13 or 5.3.23, which will be available soon.

Affected Software/OS
PHP version before 5.3.23 and 5.4.x before 5.4.13

Vulnerability Insight
Multiple flaws are due to:
- Does not validate 'soap.wsdl_cache_dir' directive before writing SOAP wsdl cache files to the filesystem.
- Allows the use of external entities while parsing SOAP wsdl files, issue in 'soap_xmlParseFile' and 'soap_xmlParseMemory' functions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - Mar13 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803337
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10

... continues on next page ...

... continued from previous page ...

Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

cve: CVE-2013-1635
cve: CVE-2013-1643
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/58224
url: http://bugs.php.net/bug.php?id=64360
url: http://cxsecurity.com/cveshow/CVE-2013-1635
url: http://cxsecurity.com/cveshow/CVE-2013-1643
url: http://bugs.gentoo.org/show_bug.cgi?id=459904
cert-bund: WID-SEC-2023-1286
cert-bund: CB-K13/1037
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2013-2065
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-1446
dfn-cert: DFN-CERT-2013-1445
dfn-cert: DFN-CERT-2013-1444
dfn-cert: DFN-CERT-2013-1392
dfn-cert: DFN-CERT-2013-1347
dfn-cert: DFN-CERT-2013-1179
dfn-cert: DFN-CERT-2013-0664
dfn-cert: DFN-CERT-2013-0481

High (CVSS: 7.5)
NVT: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Windows

Product detection result

cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Vulnerability Detection Result

Installed version: 5.3.10
Fixed version: 7.3.27
Installation
path / port: 8585/tcp

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Affected Software/OS
PHP versions prior to 7.3.27, 7.4.x prior to 7.4.15 and 8.0.x prior to 8.0.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145324
Version used: `2021-11-29T15:00:35Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2021-21702`
`url: https://www.php.net/ChangeLog-7.php#7.3.27`
`url: https://www.php.net/ChangeLog-7.php#7.4.15`
`url: https://www.php.net/ChangeLog-8.php#8.0.2`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2022-2113`
`cert-bund: CB-K21/0124`
`dfn-cert: DFN-CERT-2023-1600`
`dfn-cert: DFN-CERT-2022-2639`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2022-0904`
`dfn-cert: DFN-CERT-2021-2373`
`dfn-cert: DFN-CERT-2021-1645`
`dfn-cert: DFN-CERT-2021-1509`
`dfn-cert: DFN-CERT-2021-1453`
`dfn-cert: DFN-CERT-2021-0556`
`dfn-cert: DFN-CERT-2021-0380`
`dfn-cert: DFN-CERT-2021-0246`

High (CVSS: 7.5)
NVT: PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.39
Installation
path / port: 8585/tcp

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

Solution:
Solution type: VendorFix
Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Affected Software/OS
PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.26 and 7.2.x before 7.2.14.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.108506
Version used: 2022-08-31T10:10:28Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-19935
url: https://bugs.php.net/bug.php?id=77020
url: http://www.securityfocus.com/bid/106143
cert-bund: WID-SEC-2022-2128
cert-bund: CB-K18/1154
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2019-1181
dfn-cert: DFN-CERT-2019-0313

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-0044
dfn-cert: DFN-CERT-2018-2476

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.

Vulnerability Detection Result
We could upload the following files via the PUT method at this web server:
http://ip-10-0-0-21.us-east-2.compute.internal:8585/uploads/puttest1696587661.ht
↪ml
We could delete the following files via the DELETE method at this web server:
http://ip-10-0-0-21.us-east-2.compute.internal:8585/uploads/puttest1696587661.ht
↪ml

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.

Affected Software/OS
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method
Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Details: Test HTTP dangerous methods
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: 2022-05-12T09:32:01Z

References
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001

High (CVSS: 7.5)
NVT: PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an information disclosure vulnerability in libcurl.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.32
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.32, 7.3.20, 7.4.8 or later.

Affected Software/OS
PHP versions prior 7.2.32, 7.3 prior 7.3.20 and 7.4 prior to 7.4.8.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.144246
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-8169
url: https://www.php.net/ChangeLog-7.php#7.2.32
url: https://www.php.net/ChangeLog-7.php#7.3.20
url: https://www.php.net/ChangeLog-7.php#7.4.8
cert-bund: WID-SEC-2023-1636
cert-bund: WID-SEC-2023-1350
cert-bund: CB-K20/0684
cert-bund: CB-K20/0619
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-0807

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2020-1347

High (CVSS: 7.5)
NVT: PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial-of-service vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.30
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Affected Software/OS
PHP versions prior 7.2.30, 7.3 prior 7.3.17 and 7.4 prior to 7.4.5.

Vulnerability Insight
If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC encoding support), an out-of-bounds read can occur using a malformed url-encoded string.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.143723
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-7067

... continues on next page ...

... continued from previous page ...

```
url: https://www.php.net/ChangeLog-7.php#7.2.30
url: https://www.php.net/ChangeLog-7.php#7.3.17
url: https://www.php.net/ChangeLog-7.php#7.4.5
cert-bund: CB-K20/1199
cert-bund: CB-K20/0336
dfn-cert: DFN-CERT-2020-1438
dfn-cert: DFN-CERT-2020-0851
dfn-cert: DFN-CERT-2020-0751
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Dec18 (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     5.6.39
Installation
path / port:       8585/tcp
```

Impact

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

Solution:

Solution type: VendorFix

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

Affected Software/OS

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

Vulnerability Insight

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Vulnerabilities - Dec18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.108508
Version used: 2022-04-20T03:02:11Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-19518
cve: CVE-2018-20783
cve: CVE-2018-19395
cve: CVE-2018-19396
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
cert-bund: CB-K18/1118
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2020-0898
dfn-cert: DFN-CERT-2019-2283
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2019-1181
dfn-cert: DFN-CERT-2019-1052
dfn-cert: DFN-CERT-2019-0804
dfn-cert: DFN-CERT-2019-0698
dfn-cert: DFN-CERT-2019-0440
dfn-cert: DFN-CERT-2018-2488
dfn-cert: DFN-CERT-2018-2476

High (CVSS: 7.5)
NVT: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

Summary
PHP is improperly validating input from untrusted input.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: None`
`Installation path / port: 8585/tcp`

Solution:
Solution type: WillNotFix
No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Affected Software/OS
All PHP versions since 4.3.0 up to the latest 7.x versions.
Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively.

Vulnerability Insight
main/streams/xp_socket.c in PHP misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108875
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-7189`
`url: https://bugs.php.net/bug.php?id=74192`
`url: https://bugs.php.net/bug.php?id=74429`

... continues on next page ...

... continued from previous page ...

url: https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d5
↪95a

High (CVSS: 7.5)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.0

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

Solution:
Solution type: VendorFix
Update to PHP version 5.6.0

Affected Software/OS
PHP versions prior to 5.6.0 on Windows

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Fileinfo Component Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.808668
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2014-0236

... continues on next page ...

... continued from previous page ...

url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/90957

High (CVSS: 7.5)
NVT: PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.37
Installation
path / port: 8585/tcp

Impact
Successful exploitation will allow attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:
Solution type: VendorFix
Update 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
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (W.
↪..
OID:1.3.6.1.4.1.25623.1.0.813597

... continues on next page ...

... continued from previous page ...

Version used: 2021-08-10T15:24:26Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-14851
cve: CVE-2018-14883
cve: CVE-2018-15132
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
cert-bund: WID-SEC-2022-2130
cert-bund: CB-K18/0838
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-2116
dfn-cert: DFN-CERT-2018-1882
dfn-cert: DFN-CERT-2018-1835
dfn-cert: DFN-CERT-2018-1834
dfn-cert: DFN-CERT-2018-1777
dfn-cert: DFN-CERT-2018-1655

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities (Jun/Aug 2014) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.29
Installation
path / port: 8585/tcp

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions 5.3.x before 5.3.29, 5.4.x before 5.4.30 and 5.5.x before 5.5.14.

Vulnerability Insight
The following vulnerabilities exist:
- Fixed bug #67390 (insecure temporary file use in the configure script). (CVE-2014-3981).
- Fixed bug #67498 (phpinfo() Type Confusion Information Leak Vulnerability). (CVE-2014-4721).
- Fixed bug #67326 (cdf_read_short_sector insufficient boundary check). (CVE-2014-0207).
- Fixed bug #67410 (mconvert incorrect handling of truncated pascal string size). (CVE-2014-3478).
- Fixed bug #67411 (cdf_check_stream_offset insufficient boundary check). (CVE-2014-3479).
- Fixed bug #67412 (cdf_count_chain insufficient boundary check). (CVE-2014-3480).
- Fixed bug #67413 (cdf_read_property_info insufficient boundary check). (CVE-2014-3487).
- Fixed bug #67432 (Fix potential segfault in dns_get_record()). (CVE-2014-4049).
- Fixed bug #67492 (unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion). (CVE-2014-3515).
- Fixed bug #67397 (Buffer overflow in locale_get_display_name and uloc_getDisplayName (libicu 4.8.1)). (CVE-2014-9912).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities (Jun/Aug 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.809735
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2014-3981`
`cve: CVE-2014-4721`
`cve: CVE-2014-0207`
`cve: CVE-2014-3478`
`cve: CVE-2014-3479`
`cve: CVE-2014-3480`
`cve: CVE-2014-3487`
`cve: CVE-2014-4049`
`cve: CVE-2014-3515`
`cve: CVE-2014-9912`
`url: http://php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/67837`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/68423
url: http://www.securityfocus.com/bid/68239
url: http://www.securityfocus.com/bid/68237
url: http://www.securityfocus.com/bid/68243
url: http://www.securityfocus.com/bid/68120
url: http://www.securityfocus.com/bid/68241
url: http://www.securityfocus.com/bid/68238
url: https://bugs.php.net/bug.php?id=67390
url: https://bugs.php.net/bug.php?id=67498
url: https://bugs.php.net/bug.php?id=67326
url: https://bugs.php.net/bug.php?id=67410
url: https://bugs.php.net/bug.php?id=67411
url: https://bugs.php.net/bug.php?id=67412
url: https://bugs.php.net/bug.php?id=67413
url: https://bugs.php.net/bug.php?id=67432
url: https://bugs.php.net/bug.php?id=67492
url: https://bugs.php.net/bug.php?id=67397
url: http://seclists.org/fulldisclosure/2014/Jun/21
url: https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html
url: http://secunia.com/advisories/59575
cert-bund: CB-K17/0269
cert-bund: CB-K17/0053
cert-bund: CB-K16/0944
cert-bund: CB-K15/1704
cert-bund: CB-K15/1405
cert-bund: CB-K15/0774
cert-bund: CB-K15/0493
cert-bund: CB-K14/1359
cert-bund: CB-K14/1267
cert-bund: CB-K14/1214
cert-bund: CB-K14/1174
cert-bund: CB-K14/1167
cert-bund: CB-K14/1130
cert-bund: CB-K14/1110
cert-bund: CB-K14/0973
cert-bund: CB-K14/0972
cert-bund: CB-K14/0938
cert-bund: CB-K14/0866
cert-bund: CB-K14/0849
cert-bund: CB-K14/0842
cert-bund: CB-K14/0834
cert-bund: CB-K14/0830
cert-bund: CB-K14/0829
cert-bund: CB-K14/0818
cert-bund: CB-K14/0805
cert-bund: CB-K14/0776
cert-bund: CB-K14/0750
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0274
dfn-cert: DFN-CERT-2017-0058
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2015-1799
dfn-cert: DFN-CERT-2015-1487
dfn-cert: DFN-CERT-2015-0815
dfn-cert: DFN-CERT-2014-1434
dfn-cert: DFN-CERT-2014-1333
dfn-cert: DFN-CERT-2014-1280
dfn-cert: DFN-CERT-2014-1219
dfn-cert: DFN-CERT-2014-1181
dfn-cert: DFN-CERT-2014-1166
dfn-cert: DFN-CERT-2014-1014
dfn-cert: DFN-CERT-2014-1013
dfn-cert: DFN-CERT-2014-0982
dfn-cert: DFN-CERT-2014-0908
dfn-cert: DFN-CERT-2014-0887
dfn-cert: DFN-CERT-2014-0880
dfn-cert: DFN-CERT-2014-0870
dfn-cert: DFN-CERT-2014-0868
dfn-cert: DFN-CERT-2014-0867
dfn-cert: DFN-CERT-2014-0857
dfn-cert: DFN-CERT-2014-0839
dfn-cert: DFN-CERT-2014-0816
dfn-cert: DFN-CERT-2014-0782
```

High (CVSS: 7.5)
NVT: WordPress Multiple Vulnerabilities (Aug 2022) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.6.1
Fixed version:     4.6.24
Installation
path / port:       /wordpress
```

Solution:
Solution type: VendorFix
Update to version 3.7.39, 3.8.39, 3.9.37, 4.0.36, 4.1.36, 4.2.33, 4.3.29, 4.4.28, 4.5.27, 4.6.24, 4.7.24, 4.8.20, 4.9.21, 5.0.17, 5.1.14, 5.2.16, 5.3.13, 5.4.11, 5.5.10, 5.6.9, 5.7.7, 5.8.5, 5.9.4, 6.0.2 or later.

Affected Software/OS
WordPress version 6.0.1 and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following vulnerabilities exist:
- No CVE: SQL injection (SQLi) within the Link API
- No CVE: Cross-site scripting (XSS) on the Plugins screen
- No CVE: Output escaping issue within the_meta()

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (Aug 2022) - Windows`
OID:1.3.6.1.4.1.25623.1.0.148653
Version used: `2023-03-01T10:20:05Z`

References
`url: https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/`

High (CVSS: 7.5)
NVT: WordPress 'load-scripts.php' DoS Vulnerability - Windows

Summary
WordPress is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     NoneAvailable
Installation
path / port:       /wordpress
```

Impact
Successful exploitation will allow remote attackers to conduct a denial of service condition on affected system.

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
WordPress versions 4.9.2 and prior.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw exists as the file 'load-scripts.php' do not require any authentication and file selectively calls required JavaScript files by passing their names into the 'load' parameter, separated by a comma.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress 'load-scripts.php' DoS Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.812692
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2018-6389`
`url: https://thehackernews.com/2018/02/wordpress-dos-exploit.html`
`url: https://baraktawily.blogspot.in/2018/02/how-to-dos-29-of-world-wide-website`
`↪s.html`

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Windows

Product detection result
`cpe:/a:apache:http_server:2.2.21`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

Summary
Apache HTTP Server is prone to a NULL pointer dereference vulnerability.

Vulnerability Detection Result
`Installed version: 2.2.21`
`Fixed version: 2.4.48`
`Installation`
`path / port: 8585/tcp`

Impact
Successful exploitation will allow an attacker to crash the server.

Solution:
Solution type: VendorFix
Update to version 2.4.48 or later.

Affected Software/OS
Apache HTTP Server before version 2.4.48 on Windows.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicating why the request was rejected.
This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.112904
Version used: `2021-08-24T09:01:06Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.21`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2021-31618`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K21/0611`
`dfn-cert: DFN-CERT-2021-1549`
`dfn-cert: DFN-CERT-2021-1467`
`dfn-cert: DFN-CERT-2021-1355`
`dfn-cert: DFN-CERT-2021-1333`
`dfn-cert: DFN-CERT-2021-1329`
`dfn-cert: DFN-CERT-2021-1276`
`dfn-cert: DFN-CERT-2021-1273`

High (CVSS: 7.5)
NVT: PHP 'gdImageScaleTwoPass()' Multiple Denial of Service Vulnerabilities (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version:     5.6.12`

... continues on next page ...

... continued from previous page ...

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

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

Affected Software/OS
PHP versions prior to 5.6.12 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'gdImageScaleTwoPass()' Multiple Denial of Service Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808610
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2015-8877`
`cve: CVE-2015-8879`
`cve: CVE-2015-8874`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/90866`
`url: http://www.securityfocus.com/bid/90842`
`url: http://www.securityfocus.com/bid/90714`
`cert-bund: CB-K17/1252`
`cert-bund: CB-K16/1776`
`cert-bund: CB-K16/0975`
`cert-bund: CB-K16/0965`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K16/0937`
`cert-bund: CB-K16/0912`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0911
cert-bund: CB-K16/0868
cert-bund: CB-K16/0805
cert-bund: CB-K16/0801
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2016-1882
dfn-cert: DFN-CERT-2016-1033
dfn-cert: DFN-CERT-2016-1022
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0996
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0944
dfn-cert: DFN-CERT-2016-0924
dfn-cert: DFN-CERT-2016-0876
dfn-cert: DFN-CERT-2016-0871
dfn-cert: DFN-CERT-2016-0857
dfn-cert: DFN-CERT-2016-0855

High (CVSS: 7.5)
NVT: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.6.31 or later.

Affected Software/OS
PHP versions before 5.6.31.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)
OID:1.3.6.1.4.1.25623.1.0.811485
Version used: 2021-09-16T13:01:47Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2017-11143
url: http://www.php.net/ChangeLog-5.php
cert-bund: CB-K18/0048
cert-bund: CB-K17/1461
cert-bund: CB-K17/1358
cert-bund: CB-K17/1132
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0055
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1161

High (CVSS: 7.5)
NVT: WordPress Multiple Vulnerabilities (Oct 2022) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.25
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 3.7.40, 3.8.40, 3.9.39, 4.0.37, 4.1.37, 4.2.34, 4.3.30, 4.4.29, 4.5.28, 4.6.25, 4.7.25, 4.8.21, 4.9.22, 5.0.18, 5.1.15, 5.2.17, 5.3.14, 5.4.12, 5.5.11, 5.6.10, 5.7.8, 5.8.6, 5.9.5, 6.0.3 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress version 6.0.2 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- No CVE: Stored cross-site scripting (XSS) via wp-mail.php (post by email)
- No CVE: Open redirect in 'wp_nonce_ays'
- CVE-2022-43504: Sender's email address is exposed in wp-mail.php
- No CVE: Reflected XSS via SQL injection (SQLi) in Media Library
- No CVE: Cross-site request forgery (CSRF) in wp-trackback.php
- No CVE: Stored XSS via the Customizer
- No CVE: Revert shared user instances introduced in 50790
- No CVE: Stored XSS in WordPress Core via comment editing
- No CVE: Data exposure via the REST Terms/Tags endpoint
- No CVE: Content from multipart emails leaked
- No CVE: SQL injection (SQLi) due to improper sanitization in 'WP_Date_Query'
- No CVE: Stored XSS in the RSS Widget
- No CVE: Stored XSS in the search block
- No CVE: XSS in the Feature Image Block
- No CVE: Stored XSS in the RSS Block
- No CVE: Fix widget block XSS
Note: It is currently unclear which of the XSS vulnerabilities are related to CVE-2022-43497 and CVE-2022-43500 so these two haven't been assigned to any of the 'No CVE' tagged flaws above.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (Oct 2022) - Windows`
OID:1.3.6.1.4.1.25623.1.0.170196
Version used: `2023-05-22T12:17:59Z`

References
`cve: CVE-2022-43497`
`cve: CVE-2022-43500`
`cve: CVE-2022-43504`
`url: https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/`
`cert-bund: WID-SEC-2022-1788`

High (CVSS: 7.5)
NVT: PHP Denial of Service Vulnerability Jul17 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary

... continues on next page ...

... continued from previous page ...

PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Affected Software/OS
PHP versions before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service Vulnerability Jul17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811486
Version used: `2021-09-10T08:01:37Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-11142`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.php.net/ChangeLog-7.php`
`cert-bund: CB-K18/0048`
`cert-bund: CB-K17/1461`
`cert-bund: CB-K17/1132`
`dfn-cert: DFN-CERT-2018-0055`
`dfn-cert: DFN-CERT-2017-1529`
`dfn-cert: DFN-CERT-2017-1161`

High (CVSS: 7.5)
NVT: PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a heap buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.6.32
Installation
path / port: 8585/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
Update 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 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812072
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2017-16642
url: http://php.net/ChangeLog-5.php

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/101745
url: http://php.net/ChangeLog-7.php
url: https://bugs.php.net/bug.php?id=75055
cert-bund: CB-K18/0270
cert-bund: CB-K18/0048
cert-bund: CB-K17/2123
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0290
dfn-cert: DFN-CERT-2018-0055
dfn-cert: DFN-CERT-2017-2219

High (CVSS: 7.5)
NVT: PHP 'phar/tar.c' Heap Buffer Overflow Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a heap buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.14/5.4.4

Impact
Successful exploitation could allow attackers to execute arbitrary code or cause a denial-of-service condition via specially crafted TAR file.

Solution:
Solution type: VendorFix
Update to PHP 5.4.4 or 5.3.14 or later.

Affected Software/OS
PHP version before 5.3.14 and 5.4.x before 5.4.4

Vulnerability Insight
Flaw related to overflow in phar_parse_tarfile()function in ext/phar/tar.c in the phar extension.

Vulnerability Detection Method
Details: PHP 'phar/tar.c' Heap Buffer Overflow Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803342

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-2386
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/47545
url: http://en.securitylab.ru/nvd/426726.php
url: http://secunia.com/advisories/cve_reference/CVE-2012-2386
dfn-cert: DFN-CERT-2012-1316
dfn-cert: DFN-CERT-2012-1289
dfn-cert: DFN-CERT-2012-1288
dfn-cert: DFN-CERT-2012-1287
dfn-cert: DFN-CERT-2012-1280
dfn-cert: DFN-CERT-2012-1279
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1162
dfn-cert: DFN-CERT-2012-1100
dfn-cert: DFN-CERT-2012-1067

High (CVSS: 7.3)
NVT: PHP Multiple Vulnerabilities - 01 - Mar16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
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

... continues on next page ...

... continued from previous page ...

Update to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Mar16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807088
Version used: `2022-08-08T10:24:51Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2015-6831`
`cve: CVE-2015-6832`
`cve: CVE-2015-6833`
`url: https://bugs.php.net/bug.php?id=70068`
`url: http://www.securityfocus.com/bid/76737`
`url: http://www.securityfocus.com/bid/76739`
`url: http://www.securityfocus.com/bid/76735`
`url: http://www.openwall.com/lists/oss-security/2015/08/19/3`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K16/0422`
`cert-bund: CB-K15/1571`
`cert-bund: CB-K15/1439`
`cert-bund: CB-K15/1415`
`cert-bund: CB-K15/1261`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2016-0460`
`dfn-cert: DFN-CERT-2015-1658`
`dfn-cert: DFN-CERT-2015-1515`
`dfn-cert: DFN-CERT-2015-1493`
`dfn-cert: DFN-CERT-2015-1335`

High (CVSS: 7.3)
NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Affected Software/OS
PHP versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.807091
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-6836
url: http://www.php.net/ChangeLog-5.php

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/76644
url: https://bugs.php.net/bug.php?id=70388
cert-bund: CB-K16/0944
cert-bund: CB-K16/0422
cert-bund: CB-K15/1571
cert-bund: CB-K15/1561
cert-bund: CB-K15/1478
cert-bund: CB-K15/1439
cert-bund: CB-K15/1415
cert-bund: CB-K15/1337
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0460
dfn-cert: DFN-CERT-2015-1658
dfn-cert: DFN-CERT-2015-1644
dfn-cert: DFN-CERT-2015-1556
dfn-cert: DFN-CERT-2015-1515
dfn-cert: DFN-CERT-2015-1493
dfn-cert: DFN-CERT-2015-1407
```

High (CVSS: 7.2)
NVT: WordPress <= 4.9.8 Multiple Vulnerabilities - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.6.1
Fixed version:     None
Installation
path / port:       /wordpress
```

Impact
- CVE-2018-14028: Successful exploitation will allow remote attackers to upload php files in a predictable wp-content/uploads location and execute them.
- CVE-2018-1000773: An attacker may leverage this issue to upload arbitrary files to the affected computer. This can result in arbitrary code execution within the context of the vulnerable application.

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

... continues on next page ...

... continued from previous page ...

All WordPress versions through 4.9.8.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2018-14028: Plugins uploaded via the admin area are not verified as being ZIP files.
- CVE-2018-1000773: An input validation vulnerability in thumbnail processing that can result in remote code execution due to an incomplete fix for CVE-2017-1000600.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress <= 4.9.8 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.813910
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2018-14028`
`cve: CVE-2018-1000773`
`url: https://rastating.github.io/unrestricted-file-upload-via-plugin-uploader-in-wordpress`
`url: https://core.trac.wordpress.org/ticket/44710`
`url: https://github.com/rastating/wordpress-exploit-framework/pull/52`
`url: http://www.securityfocus.com/bid/105306`
`url: https://www.theregister.co.uk/2018/08/20/php_unserialisation_wordpress_vuln/`

High (CVSS: 7.2)
NVT: WordPress Multiple Vulnerabilities (Jan 2022) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     4.6.22
Installation
path / port:       /wordpress
```

Solution:
Solution type: VendorFix
Update to version 3.7.37, 3.8.37, 3.9.35, 4.0.34, 4.1.34, 4.2.31, 4.3.27, 4.4.26, 4.5.25, 4.6.22, 4.7.22, 4.8.18, 4.9.19, 5.0.15, 5.1.12, 5.2.14, 5.3.11, 5.4.9, 5.5.8, 5.6.7, 5.7.5, 5.8.3 or later.

Affected Software/OS
WordPress version 5.8.2 and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-21661: SQL injection (SQLi) through WP_Query
- CVE-2022-21662: Stored XSS through authenticated users
- CVE-2022-21663: Authenticated object injection in multisites
- CVE-2022-21664: SQL injection (SQLi) due to improper sanitization in WP_Meta_Query

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (Jan 2022) - Windows`
OID:1.3.6.1.4.1.25623.1.0.147397
Version used: `2023-03-01T10:20:05Z`

References
```
cve: CVE-2022-21661
cve: CVE-2022-21662
cve: CVE-2022-21663
cve: CVE-2022-21664
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-667
↪6-cqfm-gw84
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699
↪q-3hj9-889w
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmm
↪q-m8p8-332h
url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3
↪p-gw8h-6x86
cert-bund: CB-K22/0008
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2022-0027
```

High (CVSS: 7.2)
NVT: WordPress Ninja Forms Plugin < 3.6.4 SQLi Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.6.4
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.6.4 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress Ninja Forms plugin prior to version 3.6.4.

Vulnerability Insight
The plugin does not escape keys of the fields POST parameter, which could allow high privilege users to perform SQL injections attacks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.6.4 SQLi Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147258
Version used: `2022-07-20T10:33:02Z`

References
`cve: CVE-2021-24889`
`url: https://wpscan.com/vulnerability/55008a42-eb56-436c-bce0-10ee616d0495`

High (CVSS: 7.1)
NVT: PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service (DoS) and an information disclosure vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update to version 5.4.44, 5.5.28, 5.6.12, 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.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due an error in the 'make_http_soap_request' function of the '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' DoS / Information Disclosure Vulnerability - Windo.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808667
Version used: `2021-10-07T10:33:09Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-3185`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.php.net/ChangeLog-7.php`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K16/0912`
`cert-bund: CB-K16/0623`
`cert-bund: CB-K16/0614`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2016-0972`
`dfn-cert: DFN-CERT-2016-0676`
`dfn-cert: DFN-CERT-2016-0659`

High (CVSS: 7.0)
NVT: PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP released new versions which includes a security fix.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 7.3.32 (not released yet)`
`Installation`
`path / port: 8585/tcp`

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Affected Software/OS
PHP versions 5.3.7 through 7.3.31, 7.4.x through 7.4.24 and 8.0.x through 8.0.11.
Note: While the referenced CVE is only listing PHP 7.3.x, 7.4.x and 8.0.x as affected the security research team is stating in the linked blog post that all versions down to 5.3.7 are affected.

Vulnerability Insight
Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) -. ↪..`
OID:1.3.6.1.4.1.25623.1.0.117753
Version used: `2021-11-05T03:03:34Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2021-21703`
`url: https://www.php.net/ChangeLog-7.php#7.3.32`
`url: https://www.php.net/ChangeLog-7.php#7.4.25`
`url: https://www.php.net/ChangeLog-8.php#8.0.12`
`url: http://bugs.php.net/81026`
`url: https://www.ambionics.io/blog/php-fpm-local-root`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2022-0624`
`cert-bund: WID-SEC-2022-0586`
`cert-bund: CB-K21/1106`
`dfn-cert: DFN-CERT-2023-1600`
`dfn-cert: DFN-CERT-2022-2639`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2022-2337`
`dfn-cert: DFN-CERT-2022-1493`
`dfn-cert: DFN-CERT-2022-1046`
`dfn-cert: DFN-CERT-2022-0485`
`dfn-cert: DFN-CERT-2021-2586`
`dfn-cert: DFN-CERT-2021-2474`
`dfn-cert: DFN-CERT-2021-2200`

[return to 10.0.0.21]

2.1.7 High 8020/tcp

High (CVSS: 7.5)
NVT: '/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8020/.//WEB-INF/w
↪eb.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
```

... continues on next page ...

... continued from previous page ...

```
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and/or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
The following vendor fixes are known:
- Update to Payara Platform Enterprise 5.31.0, Payara Platform Community 5.2021.7 or later.
For other products please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Payara Platform Enterprise / Community
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/.//WEB-INF/web.xml
http://example.com/.//web-inf/web.xml
(note the './/' before 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: `2023-03-06T10:19:58Z`

References
`cve: CVE-2021-41381`
`url: https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-`

... continues on next page ...

... continued from previous page ...

↪054.txt
url: http://packetstormsecurity.com/files/164365/Payara-Micro-Community-5.2021.6
↪-Directory-Traversal.html

[return to 10.0.0.21]

2.1.8 High 1617/tcp

High (CVSS: 7.5)
NVT: Java JMX Insecure Configuration Vulnerability

Summary
The Java JMX interface is configured in an insecure way by allowing unauthenticated attackers to load classes from any remote URL.

Vulnerability Detection Result
It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the
↪ RMI port 49186/tcp without providing any credentials.

Solution:
Solution type: Mitigation
Enable password authentication and/or SSL client certificate authentication for the JMX agent.

Vulnerability Detection Method
Sends crafted RMI requests and checks the responses.
Details: Java JMX Insecure Configuration Vulnerability
OID:1.3.6.1.4.1.25623.1.0.143207
Version used: 2020-11-10T09:46:51Z

References
url: https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/
url: https://www.optiv.com/blog/exploiting-jmx-rmi
url: https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server

[return to 10.0.0.21]

2.1.9 High 9200/tcp

High (CVSS: 10.0)
NVT: Elasticsearch End of Life (EOL) Detection

Summary
The Elasticsearch version on the remote host has reached the End of Life (EOL) and should not be used anymore.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The "Elasticsearch" version on the remote host has reached the end of life.
CPE: cpe:/a:elastic:elasticsearch:1.1.1
Installed version: 1.1.1
EOL version: 1.1
EOL date: 2015-09-25

Impact
An EOL version of Elasticsearch 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 Elasticsearch to a version that still receives technical support and updates.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: Elasticsearch End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.113131
Version used: 2021-01-18T10:09:47Z

References
url: https://www.elastic.co/support/eol

High (CVSS: 9.8)
NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)

Summary
Elasticsearch is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 1.6.1

Impact
Successful exploitation will allow remote attackers to execute code or read arbitrary files.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.6.1, or later.

Affected Software/OS
Elasticsearch version 1.0.0 through 1.6.0 on Windows.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The Flaw is due to:
- an error in the snapshot API calls (CVE-2015-5531)
- an attack that can result in remote code execution (CVE-2015-5377).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808091
Version used: `2022-04-13T13:17:10Z`

References
`cve: CVE-2015-5531`
`cve: CVE-2015-5377`
`url: https://www.elastic.co/community/security/`
`url: http://www.securityfocus.com/bid/75935`
`url: http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded`
`cert-bund: CB-K15/1118`
`dfn-cert: DFN-CERT-2015-1160`

High (CVSS: 8.8)
NVT: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability (Windows)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result
`Installed version: 1.1.1`
`Fixed version: 5.6.12`

Impact
Successful exploitation would allow an authenticated attacker to acquire valid login credentials.

Solution:
Solution type: VendorFix
Update to version 5.6.12 or 6.4.1 respectively.

Affected Software/OS
Elasticsearch versions through 5.6.11 and 6.0.0 through 6.4.0.

Vulnerability Insight
The _cluster/settings API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability (Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.113276
Version used: `2021-05-28T04:00:18Z`

References
`cve: CVE-2018-3831`
`url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update`
`↪/149035`
`url: https://www.elastic.co/community/security`
`dfn-cert: DFN-CERT-2020-1653`

[return to 10.0.0.21]

2.1.10 High 445/tcp

High (CVSS: 8.1)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

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

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

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

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: 2023-07-14T16:09:27Z

References
cve: CVE-2017-0143
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448

[return to 10.0.0.21]

2.1.11 High 3306/tcp

High (CVSS: 10.0)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to a vulnerability in libcurl.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.41
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior and 8.0 through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149170
Version used: 2023-01-20T10:11:50Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-32221
cve: CVE-2022-35260
cve: CVE-2022-42915
cve: CVE-2022-42916
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL
advisory-id: cpujan2023
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1026
cert-bund: WID-SEC-2023-0296
cert-bund: WID-SEC-2023-0189
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0126

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1862
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0278
dfn-cert: DFN-CERT-2023-0216
dfn-cert: DFN-CERT-2023-0214
dfn-cert: DFN-CERT-2023-0157
dfn-cert: DFN-CERT-2023-0156
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2401
dfn-cert: DFN-CERT-2022-2400
dfn-cert: DFN-CERT-2022-2393
dfn-cert: DFN-CERT-2022-2391

High (CVSS: 10.0)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a vulnerability in InnoDB (zlib).

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.42
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.149536
Version used: 2023-04-19T10:19:33Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-37434
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1031
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0140
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2023-0125
cert-bund: WID-SEC-2022-1888
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0929
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2421
dfn-cert: DFN-CERT-2022-2415
dfn-cert: DFN-CERT-2022-2366
dfn-cert: DFN-CERT-2022-2365
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2363
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-1841
dfn-cert: DFN-CERT-2022-1710

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (cpuoct2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow a remote user to access restricted data.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.52 and prior, 5.6 through 5.6.33 and 5.7 through 5.7.15.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in the 'Server: Security: Encryption' and 'Server: Logging' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.809386
Version used: 2021-10-13T11:01:26Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2016-5584
cve: CVE-2016-6662
cve: CVE-2016-7440
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
url: http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution
↪-Privesc-CVE-2016-6662.txt
url: https://www.exploit-db.com/exploits/40360/
cert-bund: CB-K17/0139
cert-bund: CB-K17/0055
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1714
cert-bund: CB-K16/1655
cert-bund: CB-K16/1624
cert-bund: CB-K16/1448
cert-bund: CB-K16/1392
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1753
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1540
dfn-cert: DFN-CERT-2016-1479
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.39
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.39, 8.0.30 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.38 and prior and 8.0 through 8.0.29.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.148511
Version used: 2022-07-22T10:11:18Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-1292
cve: CVE-2022-27778
cve: CVE-2018-25032
cve: CVE-2022-21515
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixMSQL
advisory-id: cpujul2022
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0141
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1057

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0736
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0277
cert-bund: WID-SEC-2022-0071
cert-bund: WID-SEC-2022-0005
cert-bund: CB-K22/0619
cert-bund: CB-K22/0570
cert-bund: CB-K22/0536
cert-bund: CB-K22/0386
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2066
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1992
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1875
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1614
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1476
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1310
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1049
dfn-cert: DFN-CERT-2022-0986
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716
```

High (CVSS: 9.8)
NVT: Oracle Mysql Security Update (cpuoct2018 - 02) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL version 5.5.x through 5.5.61, 5.6.x through 5.6.41, 5.7.x through 5.7.23 and 8.0.x through 8.0.12.

Vulnerability Insight
Multiple flaws exist due to:
- An unspecified error within 'InnoDB (zlib)' component of MySQL Server.
- An unspecified error within 'Server: Parser' component of MySQL Server.
- An unspecified error within 'Client programs' component of MySQL Server.
- An unspecified error within 'Server: Storage Engines' component of MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Update (cpuoct2018 - 02) - Windows`
OID:1.3.6.1.4.1.25623.1.0.814258
Version used: `2022-06-24T09:38:38Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2018-3133`
`cve: CVE-2018-3174`
`cve: CVE-2018-3282`
`cve: CVE-2016-9843`
`cve: CVE-2016-9840`
`cve: CVE-2016-9841`
`cve: CVE-2016-9842`
`url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL`
`advisory-id: cpuoct2018`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0714`
`cert-bund: CB-K18/1005`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K18/0030`
`cert-bund: CB-K17/2199`
`cert-bund: CB-K17/2168`
`cert-bund: CB-K17/1745`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1622`
`cert-bund: CB-K17/1585`
`cert-bund: CB-K17/1062`
`cert-bund: CB-K17/0877`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/0784
cert-bund: CB-K16/1996
dfn-cert: DFN-CERT-2020-1536
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2273
dfn-cert: DFN-CERT-2018-2110
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2016-2109
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.36
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 5.7.36, 8.0.27 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.35 and prior and 8.0 through 8.0.26.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117741
Version used: `2021-10-23T08:58:44Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2021-22947`
`cve: CVE-2021-3711`
`cve: CVE-2021-22926`
`cve: CVE-2021-35604`
`cve: CVE-2021-35624`
`cve: CVE-2021-22922`
`cve: CVE-2021-22923`
`cve: CVE-2021-22924`
`cve: CVE-2021-22925`
`cve: CVE-2021-22945`
`cve: CVE-2021-22946`
`cve: CVE-2021-3712`
`url: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL`
`advisory-id: cpuoct2021`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-1030`
`cert-bund: WID-SEC-2023-0530`
`cert-bund: WID-SEC-2022-2354`
`cert-bund: WID-SEC-2022-2000`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: WID-SEC-2022-1894`
`cert-bund: WID-SEC-2022-1515`
`cert-bund: WID-SEC-2022-1461`
`cert-bund: WID-SEC-2022-1335`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0874
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0473
cert-bund: CB-K22/0469
cert-bund: CB-K22/0316
cert-bund: CB-K22/0224
cert-bund: CB-K22/0077
cert-bund: CB-K22/0072
cert-bund: CB-K22/0062
cert-bund: CB-K22/0045
cert-bund: CB-K22/0030
cert-bund: CB-K22/0011
cert-bund: CB-K21/1268
cert-bund: CB-K21/1179
cert-bund: CB-K21/1161
cert-bund: CB-K21/1087
cert-bund: CB-K21/0994
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
cert-bund: CB-K21/0907
cert-bund: CB-K21/0897
cert-bund: CB-K21/0797
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0867
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0120
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0052
dfn-cert: DFN-CERT-2022-0031
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2502
dfn-cert: DFN-CERT-2021-2481
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2434
dfn-cert: DFN-CERT-2021-2403
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2369
dfn-cert: DFN-CERT-2021-2329
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2189
dfn-cert: DFN-CERT-2021-2188
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2167
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1931
dfn-cert: DFN-CERT-2021-1917
dfn-cert: DFN-CERT-2021-1915
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1799
dfn-cert: DFN-CERT-2021-1743

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1593
dfn-cert: DFN-CERT-2021-1580
dfn-cert: DFN-CERT-2021-1568

High (CVSS: 9.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced vendor advisory or upgrade to the latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.64 and Oracle MySQL version 5.5.x to 5.5.26 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component related to server replication, information schema, protocol and server optimizer.

Vulnerability Detection Method
Details: Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803111
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2012-3197
cve: CVE-2012-3163
cve: CVE-2012-3158
cve: CVE-2012-3150
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/55990
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56017
url: http://www.securityfocus.com/bid/56036
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118

High (CVSS: 7.8)
NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
It was possible to login into the remote MySQL as root using weak credentials.

Vulnerability Detection Result
It was possible to login as root with an empty password.

Solution:
Solution type: Mitigation
- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

Affected Software/OS
The following products are know to use such weak credentials:
- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030

... continues on next page ...

... continued from previous page ...

- CVE-2009-0919: XAMPP
- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4

Other products might be affected as well.

Vulnerability Detection Method

Details: `MySQL / MariaDB Default Credentials (MySQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `2023-04-17T10:19:34Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2001-0645
cve: CVE-2004-2357
cve: CVE-2006-1451
cve: CVE-2007-2554
cve: CVE-2007-6081
cve: CVE-2009-0919
cve: CVE-2014-3419
cve: CVE-2015-4669
cve: CVE-2016-6531
cve: CVE-2018-15719
```

High (CVSS: 7.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.31 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.30.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149534
Version used: `2023-04-19T10:19:33Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2023-21912`
`url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL`
`advisory-id: cpuapr2023`
`cert-bund: WID-SEC-2023-1033`
`dfn-cert: DFN-CERT-2023-1058`
`dfn-cert: DFN-CERT-2023-1037`
`dfn-cert: DFN-CERT-2023-0885`

High (CVSS: 7.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version:     5.7.42`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.33 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149538
Version used: 2023-04-19T10:19:33Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2023-0215
cve: CVE-2022-43551
cve: CVE-2023-21980
cve: CVE-2022-4304
cve: CVE-2022-4450
cve: CVE-2023-0286
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1553
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0777
cert-bund: WID-SEC-2023-0304
cert-bund: WID-SEC-2022-2375
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-1256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-1043
dfn-cert: DFN-CERT-2023-1037
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0774
dfn-cert: DFN-CERT-2023-0685
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2023-0618
dfn-cert: DFN-CERT-2023-0543
dfn-cert: DFN-CERT-2023-0471
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0318
dfn-cert: DFN-CERT-2023-0310
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0288
dfn-cert: DFN-CERT-2023-0284
dfn-cert: DFN-CERT-2023-0283
dfn-cert: DFN-CERT-2022-2902
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.40
Installation
path / port:       3306/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Update to version 5.5.40, 5.6.21 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5.39 and prior and 5.6 through 5.6.20.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to C API SSL CERTIFICATE HANDLING, SERVER:DML, SERVER:SSL:yaSSL, SERVER:OPTIMIZER, SERVER:INNODB DML FOREIGN KEYS.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804781
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-6507`
`cve: CVE-2014-6491`
`cve: CVE-2014-6500`
`cve: CVE-2014-6469`
`cve: CVE-2014-6555`
`cve: CVE-2014-6559`
`cve: CVE-2014-6494`
`cve: CVE-2014-6496`
`cve: CVE-2014-6464`
`url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/70444`
`url: http://www.securityfocus.com/bid/70446`
`url: http://www.securityfocus.com/bid/70451`
`url: http://www.securityfocus.com/bid/70469`
`url: http://www.securityfocus.com/bid/70478`
`url: http://www.securityfocus.com/bid/70487`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/70497
url: http://www.securityfocus.com/bid/70530
url: http://www.securityfocus.com/bid/70550
advisory-id: cpuoct2014
cert-bund: CB-K15/1518
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1299
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2014-1567
dfn-cert: DFN-CERT-2014-1500
dfn-cert: DFN-CERT-2014-1357
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

Vulnerability Insight
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Option' sub-component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808591
Version used: `2022-07-07T10:16:06Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-3471`
`url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/91913`
`advisory-id: cpujul2016`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/1100`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-1169`

High (CVSS: 7.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server version 5.5.40 and earlier, and 5.6.21 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Server:-Security:Encryption, InnoDB:DML, Replication, and Security:Privileges:Foreign Key.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805132
Version used: `2022-04-14T06:42:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2015-0411`
`cve: CVE-2014-6568`
`cve: CVE-2015-0382`
`cve: CVE-2015-0381`
`cve: CVE-2015-0374`
`url: http://secunia.com/advisories/62525`
`url: http://www.securityfocus.com/bid/72191`
`url: http://www.securityfocus.com/bid/72210`
`url: http://www.securityfocus.com/bid/72200`
`url: http://www.securityfocus.com/bid/72214`
`url: http://www.securityfocus.com/bid/72227`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html`
`cert-bund: CB-K15/1193`
`cert-bund: CB-K15/0964`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K15/0415`
`cert-bund: CB-K15/0073`
`dfn-cert: DFN-CERT-2015-1264`
`dfn-cert: DFN-CERT-2015-1016`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074

High (CVSS: 7.5)
NVT: Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.21
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow attackers to cause crash of applications using that MySQL client.

Solution:
Solution type: VendorFix
Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.

Affected Software/OS
Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Windows

Vulnerability Insight
Multiple errors exist as,
- In sql-common/client.c script 'mysql_prune_stmt_list' function, the for loop adds elements to pruned_list without removing it from the existing list.
- If application gets disconnected just before it tries to prepare a new statement, 'mysql_prune_stmt_list' tries to detach all previously prepared statements.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.810603
Version used: 2021-10-12T09:28:32Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2017-3302
url: https://bugs.mysql.com/bug.php?id=63363
url: https://bugs.mysql.com/bug.php?id=70429
url: http://www.openwall.com/lists/oss-security/2017/02/11/11
cert-bund: CB-K18/0224
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430

High (CVSS: 7.5)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation of this vulnerability will allow remote attackers to cause the affected application to crash, resulting in a denial-of-service condition.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.54 and earlier, 5.6.20 and earlier on Windows

Vulnerability Insight
The flaw exists due to some unspecified error in the 'Server: C API' component due to failure to handle exceptional conditions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810880
Version used: `2023-07-14T16:09:27Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2017-3302`
`url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html`
`url: http://www.securityfocus.com/bid/96162`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/1604`
`cert-bund: CB-K17/1298`
`cert-bund: CB-K17/1239`
`cert-bund: CB-K17/0657`
`cert-bund: CB-K17/0423`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-0242`
`dfn-cert: DFN-CERT-2017-1675`
`dfn-cert: DFN-CERT-2017-1341`
`dfn-cert: DFN-CERT-2017-1282`
`dfn-cert: DFN-CERT-2017-0675`
`dfn-cert: DFN-CERT-2017-0430`

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.49
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.49 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.48 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows
OID:1.3.6.1.4.1.25623.1.0.144286
Version used: 2021-08-16T12:00:57Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2020-1967
cve: CVE-2020-14539
cve: CVE-2020-14559
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL
advisory-id: cpujul2020
cert-bund: CB-K21/1088
cert-bund: CB-K21/0070
cert-bund: CB-K20/1023
cert-bund: CB-K20/1017

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0711
cert-bund: CB-K20/0708
cert-bund: CB-K20/0357
dfn-cert: DFN-CERT-2021-2192
dfn-cert: DFN-CERT-2021-0830
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0140
dfn-cert: DFN-CERT-2020-2295
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1788
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-0956
dfn-cert: DFN-CERT-2020-0930
dfn-cert: DFN-CERT-2020-0841
dfn-cert: DFN-CERT-2020-0824
dfn-cert: DFN-CERT-2020-0822
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.38
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.38, 8.0.29 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.37 and prior and 8.0 through 8.0.28.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.113944
Version used: 2022-04-25T14:30:15Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-0778
cve: CVE-2022-21454
cve: CVE-2022-21417
cve: CVE-2022-21427
cve: CVE-2022-21451
cve: CVE-2022-21444
cve: CVE-2022-21460
url: https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixMSQL
advisory-id: cpuapr2022
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1081
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0551
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0270
cert-bund: WID-SEC-2022-0261
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0190
cert-bund: WID-SEC-2022-0169
cert-bund: WID-SEC-2022-0065
cert-bund: CB-K22/0619
cert-bund: CB-K22/0470
cert-bund: CB-K22/0468
cert-bund: CB-K22/0321

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1928
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1667
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1370
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1205
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603

High (CVSS: 7.4)
NVT: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.34
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.34, 8.0.24 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.33 and prior and 8.0 through 8.0.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145796
Version used: 2021-08-26T14:01:06Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2021-3449
cve: CVE-2021-3450
cve: CVE-2021-23840
cve: CVE-2021-23841
cve: CVE-2021-2307
cve: CVE-2021-2304
cve: CVE-2021-2180
cve: CVE-2021-2194
cve: CVE-2021-2166
cve: CVE-2021-2179
cve: CVE-2021-2226
cve: CVE-2021-2169
cve: CVE-2021-2146
cve: CVE-2021-2174
cve: CVE-2021-2171
cve: CVE-2021-2162
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1320
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1294
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0671
cert-bund: WID-SEC-2022-0669
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K22/0476
cert-bund: CB-K22/0061
cert-bund: CB-K21/1097
cert-bund: CB-K21/1095
cert-bund: CB-K21/1065
cert-bund: CB-K21/0785
cert-bund: CB-K21/0770
cert-bund: CB-K21/0573
cert-bund: CB-K21/0572
cert-bund: CB-K21/0565
cert-bund: CB-K21/0421
cert-bund: CB-K21/0412
cert-bund: CB-K21/0409
cert-bund: CB-K21/0389
cert-bund: CB-K21/0317
cert-bund: CB-K21/0185
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2197
dfn-cert: DFN-CERT-2021-2196
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1825

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1740
dfn-cert: DFN-CERT-2021-1670
dfn-cert: DFN-CERT-2021-1660
dfn-cert: DFN-CERT-2021-1549
dfn-cert: DFN-CERT-2021-1547
dfn-cert: DFN-CERT-2021-1537
dfn-cert: DFN-CERT-2021-1500
dfn-cert: DFN-CERT-2021-1418
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1132
dfn-cert: DFN-CERT-2021-1129
dfn-cert: DFN-CERT-2021-1128
dfn-cert: DFN-CERT-2021-1098
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0984
dfn-cert: DFN-CERT-2021-0884
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0829
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0818
dfn-cert: DFN-CERT-2021-0813
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0696
dfn-cert: DFN-CERT-2021-0656
dfn-cert: DFN-CERT-2021-0630
dfn-cert: DFN-CERT-2021-0629
dfn-cert: DFN-CERT-2021-0409
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2021-0363

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a vulnerability in the parser.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.30
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.30, 8.0.20 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.29 and prior and 8.0 through 8.0.19.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145800
Version used: 2021-08-26T13:01:12Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2021-2144
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2021-0821

High (CVSS: 7.2)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-06 Oct15 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary

... continues on next page ...

... continued from previous page ...

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server Server 5.5.44 and earlier, and 5.6.25 and earlier

Vulnerability Insight

Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method

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

Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-06 Oct15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805769

Version used: `2022-04-14T06:42:08Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4879
cve: CVE-2015-4819
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77140
url: http://www.securityfocus.com/bid/77196
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638
```

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.46 and prior, 5.6 through 5.6.27 and version 5.7.9.

Vulnerability Insight

Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan20.
↪..
OID:1.3.6.1.4.1.25623.1.0.806876
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-0609
cve: CVE-2016-0608
cve: CVE-2016-0606
cve: CVE-2016-0600
cve: CVE-2016-0598
cve: CVE-2016-0597
cve: CVE-2016-0546
cve: CVE-2016-0505
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81258
url: http://www.securityfocus.com/bid/81226
url: http://www.securityfocus.com/bid/81188
url: http://www.securityfocus.com/bid/81182
url: http://www.securityfocus.com/bid/81151
url: http://www.securityfocus.com/bid/81066
url: http://www.securityfocus.com/bid/81088
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0143

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0104

High (CVSS: 7.2)
NVT: Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.52
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an remote attacker to gain elevated privileges on the affected system, also could allow buffer overflow attacks.

Solution:
Solution type: VendorFix
Upgrade to Oracle MySQL Server 5.5.52 or later.

Affected Software/OS
Oracle MySQL Server 5.5.x to 5.5.51 on windows

Vulnerability Insight
Multiple errors exist. Please see the references for more information.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.809300
Version used: 2021-10-15T11:13:32Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References
url: http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html

High (CVSS: 7.1)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpujan2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

Solution:
Solution type: VendorFix
Updates are available. Apply the necessary patch from the referenced link.

Affected Software/OS
Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

Vulnerability Insight
The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.112489

... continues on next page ...

... continued from previous page ...

Version used: 2023-02-02T10:09:00Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-2534
cve: CVE-2019-2529
cve: CVE-2019-2482
cve: CVE-2019-2455
cve: CVE-2019-2503
cve: CVE-2018-0734
cve: CVE-2019-2537
cve: CVE-2019-2481
cve: CVE-2019-2507
cve: CVE-2019-2531
cve: CVE-2018-5407
url: https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL
advisory-id: cpujan2019
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-1696
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K22/0045
cert-bund: CB-K20/0324
cert-bund: CB-K20/0136
cert-bund: CB-K19/1121
cert-bund: CB-K19/0696
cert-bund: CB-K19/0622
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0318
cert-bund: CB-K19/0316
cert-bund: CB-K19/0314
cert-bund: CB-K19/0050
cert-bund: CB-K19/0044
cert-bund: CB-K18/1173
cert-bund: CB-K18/1065
cert-bund: CB-K18/1039
dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2456

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-2305
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1600
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0782
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0778
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0232
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2019-0103
dfn-cert: DFN-CERT-2019-0102
dfn-cert: DFN-CERT-2018-2541
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2513
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2444
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2360
dfn-cert: DFN-CERT-2018-2338
dfn-cert: DFN-CERT-2018-2214
```

High (CVSS: 7.1)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service attack and partially modify data.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.19 and earlier on Windows

Vulnerability Insight
The flaw exists due to an error in 'Server:Partition' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.812650
Version used: 2022-07-04T10:18:32Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2018-2562
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0480
cert-bund: CB-K18/0392
cert-bund: CB-K18/0265
cert-bund: CB-K18/0096
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0424
dfn-cert: DFN-CERT-2018-0286
dfn-cert: DFN-CERT-2018-0101

High (CVSS: 7.0)
NVT: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (cpuoct2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation of these vulnerabilities will allow remote authenticated attackers to cause denial of service conditions and gain elevated privileges.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.51 and prior, 5.6 through 5.6.32 and 5.7 through 5.7.14.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in the 'Server:GIS', 'Server:Federated', 'Server:Optimizer', 'Server:Types', 'Server:Error Handling' and 'Server:MyISAM' components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.809372

... continues on next page ...

... continued from previous page ...

Version used: 2021-10-13T11:01:26Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-3492
cve: CVE-2016-5626
cve: CVE-2016-5629
cve: CVE-2016-5616
cve: CVE-2016-5617
cve: CVE-2016-8283
cve: CVE-2016-6663
cve: CVE-2016-6664
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0139
cert-bund: CB-K16/1979
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2016-2089
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714

[return to 10.0.0.21]

2.1.12 High 4848/tcp

High (CVSS: 7.5)
NVT: Oracle Glass Fish Server Directory Traversal Vulnerability

Summary
Glass fish server is prone to a directory traversal vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable URL: https://ip-10-0-0-21.us-east-2.compute.internal:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/windows/win.ini

Impact
Successful exploitation will allow remote attackers to gain access to sensitive information.

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
Oracle Glassfish Server version 4.1.1 and probably prior.

Vulnerability Insight
The flaw is due to
- Improper sanitization of parameter 'META-INF' in 'theme.php' file.

Vulnerability Detection Method
Send a crafted request via HTTP GET and check whether it is able to get the content of passwd file.
Details: Oracle Glass Fish Server Directory Traversal Vulnerability
OID:1.3.6.1.4.1.25623.1.0.806848
Version used: 2021-10-11T08:01:31Z

References
cve: CVE-2017-1000028
url: https://www.exploit-db.com/exploits/39241

[return to 10.0.0.21]

2.1.13 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result
cpe:/a:microsoft:internet_information_services:7.5
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)

... continues on next page ...

... continued from previous page ...

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

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

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: `MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2022-12-05T10:11:03Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2015-1635`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://support.microsoft.com/kb/3042553`
`url: https://technet.microsoft.com/library/security/MS15-034`
`url: http://pastebin.com/ypURDPc4`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545
```

[return to 10.0.0.21]

2.1.14 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):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Password required for anonymous.
```

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: `2023-07-14T16:09:27Z`

[return to 10.0.0.21]

2.1.15 Medium 8383/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

... continues on next page ...

... continued from previous page ...

Summary
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Vulnerability Detection Result
```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F70
↪63656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L
↪=Pleasanton,ST=CA,C=US (Server certificate)
```

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

References
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

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 2020-09-05 12:24:44.
Certificate details:
fingerprint (SHA-1)                | 701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315
fingerprint (SHA-256)              | C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E
↪B135AD83CD7B01A5A5
```

... continues on next page ...

... continued from previous page ...

issued by	1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleasanton,ST=CA,C=US
public key algorithm	RSA
public key size (bits)	1024
serial	00F59CEF71E6DB72A5
signature algorithm	sha1WithRSAEncryption
subject	1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleasanton,ST=CA,C=US
subject alternative names (SAN)	None
valid from	2010-09-08 12:24:44 UTC
valid until	2020-09-05 12:24:44 UTC

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: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerable URL: https://ip-10-0-0-21.us-east-2.compute.internal:8383/WEB-INf./web.xml
Response (truncated):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
```

... continues on next page ...

... continued from previous page ...

```
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

The following products are known to be affected:
- A misconfigured reverse proxy.
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/META-INf./web.xml
(note the 'f.' in 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INf./' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117225
Version used: `2023-03-06T10:19:58Z`

References
`url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667`

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Vulnerable URL: https://ip-10-0-0-21.us-east-2.compute.internal:8383/WEB-INF../w
↪eb.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
```

... continues on next page ...

... continued from previous page ...

```
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Caucho Resin version 2.1.12 on Apache HTTP server version 1.3.29
Other products and versions might be affected as well.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/WEB-INF../web.xml
http://example.com/web-inf../web.xml
(note the double dot ('..') after 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INF../' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117221
Version used: `2023-06-16T05:06:18Z`

References
`cve: CVE-2004-0281`
`url: http://marc.info/?l=bugtraq&m=107635084830547&w=2`
`url: http://www.securityfocus.com/bid/9617`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

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.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ 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 TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`
`cert-bund: CB-K15/0365`
`cert-bund: CB-K15/0364`
`cert-bund: CB-K15/0302`
`cert-bund: CB-K15/0192`
`cert-bund: CB-K15/0079`
`cert-bund: CB-K15/0016`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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=#737570706F7274406465736B746F7063656E
↪7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleas
↪anton,ST=CA,C=US
```

... continues on next page ...

... continued from previous page ...

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)
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: 2021-10-15T11:13:32Z

References
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

... continues on next page ...

... continued from previous page ...

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 the references).
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.

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: `2021-02-12T06:42:15Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.0.0.21]

2.1.16 Medium 8484/tcp

Medium (CVSS: 6.5)
NVT: Jenkins < 2.146 and < 2.138.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.146
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.146 or later / Jenkins LTS to 2.138.2 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Jenkins LTS up to and including 2.138.1, Jenkins weekly up to and including 2.145.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Path traversal vulnerability in Stapler allowed accessing internal data (CVE-2018-1000997).
- Arbitrary file write vulnerability using file parameter definitions (CVE-2018-1000406).
- Reflected XSS vulnerability (CVE-2018-1000407).
- Ephemeral user record was created on some invalid authentication attempts (CVE-2018-1999043).
- Ephemeral user record creation (CVE-2018-1000408).
- Session fixation vulnerability on user signup (CVE-2018-1000409).
- Failures to process form submission data could result in secrets being displayed or written to logs (CVE-2018-1000410).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.146 and < 2.138.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.108510
Version used: `2021-10-11T09:46:29Z`

References
`cve: CVE-2018-1999043`
`cve: CVE-2018-1000406`
`cve: CVE-2018-1000407`
`cve: CVE-2018-1000408`
`cve: CVE-2018-1000409`
`cve: CVE-2018-1000410`
`cve: CVE-2018-1000997`
`url: https://jenkins.io/security/advisory/2018-10-10/`

Medium (CVSS: 5.8)
NVT: Jenkins < 2.303.2, < 2.315 Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.315
Installation
path / port:       /
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to version 2.315, 2.303.2 LTS or later.

Affected Software/OS
Jenkins version 2.314 and prior and 2.303.1 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2014-3577: Jenkins core bundles vulnerable version of the commons-httpclient library
- CVE-2021-21682: Improper handling of equivalent directory names
- CVE-2021-21683: Path traversal

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.303.2, < 2.315 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.146873
Version used: `2021-10-08T08:43:41Z`

References
`cve: CVE-2014-3577`
`cve: CVE-2021-21682`
`cve: CVE-2021-21683`
`url: https://www.jenkins.io/security/advisory/2021-10-06/`
`cert-bund: WID-SEC-2023-0432`
`cert-bund: WID-SEC-2023-0306`
`cert-bund: WID-SEC-2022-1375`
`cert-bund: CB-K16/1303`
`cert-bund: CB-K15/1508`
`cert-bund: CB-K15/1506`
`cert-bund: CB-K15/0929`
`cert-bund: CB-K15/0928`
`cert-bund: CB-K15/0678`
`cert-bund: CB-K15/0391`
`cert-bund: CB-K15/0330`
`cert-bund: CB-K15/0186`
`cert-bund: CB-K15/0148`
`cert-bund: CB-K14/1598`
`cert-bund: CB-K14/1485`
`cert-bund: CB-K14/1111`
`cert-bund: CB-K14/1035`
`dfn-cert: DFN-CERT-2022-0569`
`dfn-cert: DFN-CERT-2021-2094`
`dfn-cert: DFN-CERT-2021-1111`
`dfn-cert: DFN-CERT-2020-2385`
`dfn-cert: DFN-CERT-2016-1386`
`dfn-cert: DFN-CERT-2015-1595`
`dfn-cert: DFN-CERT-2015-1576`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0953
dfn-cert: DFN-CERT-2015-0951
dfn-cert: DFN-CERT-2015-0712
dfn-cert: DFN-CERT-2015-0403
dfn-cert: DFN-CERT-2015-0342
dfn-cert: DFN-CERT-2015-0191
dfn-cert: DFN-CERT-2015-0152
dfn-cert: DFN-CERT-2014-1693
dfn-cert: DFN-CERT-2014-1572
dfn-cert: DFN-CERT-2014-1157
dfn-cert: DFN-CERT-2014-1078
```

Medium (CVSS: 5.8)
NVT: Jenkins < 2.219, < 2.204.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.219
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 2.219, 2.204.2 LTS or later.

Affected Software/OS
Jenkins version 2.218 and prior and 2.204.1 LTS and prior.

Vulnerability Insight
Jenkins is prone to multiple vulnerabilities:
- UDP amplification reflection attack (CVE-2020-2100)
- Non-constant time comparison of inbound TCP agent connection secret (CVE-2020-2101)
- Non-constant time HMAC comparison (CVE-2020-2102)
- Diagnostic page exposed session cookies (CVE-2020-2103)
- Memory usage graphs accessible to anyone with Overall/Read (CVE-2020-2104)
- Jenkins REST APIs vulnerable to clickjacking (CVE-2020-2105)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.219, < 2.204.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.143440
Version used: `2021-07-08T11:00:45Z`

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2020-2100
cve: CVE-2020-2101
cve: CVE-2020-2102
cve: CVE-2020-2103
cve: CVE-2020-2104
cve: CVE-2020-2105
url: https://jenkins.io/security/advisory/2020-01-29/
dfn-cert: DFN-CERT-2020-0207

Medium (CVSS: 5.4)
NVT: Jenkins < 2.252, < 2.235.4 Multiple XSS Vulnerabilities - Windows

Summary
Jenkins is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.252
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 2.252, 2.235.4 LTS or later.

Affected Software/OS
Jenkins version 2.251 and prior and 2.235.3 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:
- Stored XSS vulnerability in help icons (CVE-2020-2229)
- Stored XSS vulnerability in project naming strategy (CVE-2020-2230)
- Stored XSS vulnerability in 'Trigger builds remotely' (CVE-2020-2231)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.252, < 2.235.4 Multiple XSS Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.144389
Version used: 2021-07-08T11:00:45Z

References
cve: CVE-2020-2230
cve: CVE-2020-2229
cve: CVE-2020-2231

... continues on next page ...

... continued from previous page ...

url: https://www.jenkins.io/security/advisory/2020-08-12/
cert-bund: WID-SEC-2022-1627
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-1787

Medium (CVSS: 5.4)
NVT: Jenkins < 2.138 and < 2.121.3 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.138
Installation
path / port: /

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.138 or later / Jenkins LTS to 2.121.3 or later.

Affected Software/OS
Jenkins LTS up to and including 2.121.2, Jenkins weekly up to and including 2.137.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Jenkins allowed deserialization of URL objects via Remoting (agent communication) and XStream (CVE-2018-1999042).
- Ephemeral user record was created on some invalid authentication attempts (CVE-2018-1999043).
- Cron expression form validation could enter infinite loop, potentially resulting in denial of service (CVE-2018-1999044).
- 'Remember me' cookie was evaluated even if that feature is disabled (CVE-2018-1999045).
- Unauthorized users could access agent logs (CVE-2018-1999046).
- Unauthorized users could cancel scheduled restarts initiated from the update center (CVE-2018-1999047).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.138 and < 2.121.3 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.112360
Version used: 2021-10-11T09:46:29Z

References
cve: CVE-2018-1999042
cve: CVE-2018-1999043

... continues on next page ...

... continued from previous page ...

cve: CVE-2018-1999044
cve: CVE-2018-1999045
cve: CVE-2018-1999046
cve: CVE-2018-1999047
url: https://jenkins.io/security/advisory/2018-08-15/

Medium (CVSS: 5.4)
NVT: Jenkins < 2.197 and < 2.176.4 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.197
Installation
path / port: /

Solution:
Solution type: VendorFix
Update Jenkins weekly to version 2.197 or later / Jenkins LTS to version 2.176.4 or later.

Affected Software/OS
Jenkins LTS up to and including 2.176.3, Jenkins weekly up to and including 2.196.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- The f:expandableTextBox form control interpreted its content as HTML when expanded, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents, typically Job/Configure. (CVE-2019-10401)
- The f:combobox form control interpreted its item labels as HTML, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents. (CVE-2019-10402)
- The SCM tag name on the tooltip for SCM tag actions was not being escaped, resulting in a stored XSS vulnerability exploitable by users able to control SCM tag names for these actions. (CVE-2019-10403)
- The reason why a queue item is blocked in tooltips was not being escaped, resulting in a stored XSS vulnerability exploitable by users able to control parts of the reason a queue item is blocked, such as label expressions not matching any idle executors. (CVE-2019-10404)
- The value of the 'Cookie' HTTP request header on the /whoAmI/ URL was being printed, allowing attackers exploiting another XSS vulnerability to obtain the HTTP session cookie despite it being marked as HttpOnly. (CVE-2019-10405)
- The values set as Jenkins URL in the global configuration were not being restricted or filtered, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission. (CVE-2019-10406)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.197 and < 2.176.4 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.114138
Version used: 2023-02-23T10:19:58Z

References
cve: CVE-2019-10401
cve: CVE-2019-10402
cve: CVE-2019-10403
cve: CVE-2019-10404
cve: CVE-2019-10405
cve: CVE-2019-10406
url: https://jenkins.io/security/advisory/2019-09-25/

Medium (CVSS: 5.4)
NVT: Jenkins < 2.245, < 2.235.2 LTS Multiple XSS Vulnerabilities - Windows

Summary
Jenkins is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.245
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 2.245, 2.235.2 LTS or later.

Affected Software/OS
Jenkins version 2.244 and prior and 2.235.1 LTS and prior.

Vulnerability Insight
The following vulnerabilities exist:
- Stored XSS vulnerability in job build time trend (CVE-2020-2220)
- Stored XSS vulnerability in upstream cause (CVE-2020-2221)
- Stored XSS vulnerability in 'keep forever' badge icons (CVE-2020-2222)
- Stored XSS vulnerability in console links (CVE-2020-2223)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.245, < 2.235.2 LTS Multiple XSS Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.112780
Version used: 2021-07-08T11:00:45Z

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2020-2220
cve: CVE-2020-2221
cve: CVE-2020-2222
cve: CVE-2020-2223
url: https://jenkins.io/security/advisory/2020-07-15/
dfn-cert: DFN-CERT-2020-1871
dfn-cert: DFN-CERT-2020-1851
dfn-cert: DFN-CERT-2020-1607

Medium (CVSS: 5.3)
NVT: Jenkins < 2.107 and < 2.89.4 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.107
Installation
path / port: /

Solution:
Solution type: VendorFix
Upgrade to Jenkins weekly to 2.107 or later / Jenkins LTS to 2.89.4 or later.

Affected Software/OS
Jenkins LTS up to and including 2.89.3, Jenkins weekly up to and including 2.106.

Vulnerability Insight
Jenkins is prone to the following vulnerabilities:
- Path traversal vulnerability which allows access to files outside plugin resources. (CVE-2018-6356)
- Improperly secured form validation for proxy configuration, allowing Server-Side Request Forgery. (CVE-2018-1000067)
- Improper input validation, allowing unintended access to plugin resource files on case-insensitive file systems. (CVE-2018-1000068)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.107 and < 2.89.4 LTS Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.112228
Version used: 2022-06-15T03:04:08Z

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2018-6356
cve: CVE-2018-1000067
cve: CVE-2018-1000068
url: https://jenkins.io/security/advisory/2018-02-14/
cert-bund: CB-K18/0315
dfn-cert: DFN-CERT-2018-0340

Medium (CVSS: 5.3)
NVT: Jenkins < 2.276, < 2.263.3 Arbitrary File Read Vulnerability

Summary
Jenkins is prone to an arbitrary file read vulnerability.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.276
Installation
path / port: /

Impact
The vulnerability allows attackers with Job/Workspace permission and the ability to control workspace contents, e.g., with Job/Configure permission or the ability to change SCM contents, to create symbolic links that allow them to access files outside workspaces using the workspace browser.

Solution:
Solution type: VendorFix
Update to version 2.276, 2.263.3 LTS or later.

Affected Software/OS
Jenkins version 2.275 and prior and 2.263.2 LTS and prior.

Vulnerability Insight
Due to a time-of-check to time-of-use (TOCTOU) race condition, the file browser for workspaces, archived artifacts, and $JENKINS_HOME/userContent/ follows symbolic links to locations outside the directory being browsed in Jenkins.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins < 2.276, < 2.263.3 Arbitrary File Read Vulnerability
OID:1.3.6.1.4.1.25623.1.0.145266
Version used: 2021-08-17T14:01:00Z

References
cve: CVE-2021-21615

... continues on next page ...

... continued from previous page ...

url: https://www.jenkins.io/security/advisory/2021-01-26/#SECURITY-2197
dfn-cert: DFN-CERT-2021-0376
dfn-cert: DFN-CERT-2021-0173

Medium (CVSS: 5.3)
NVT: Jenkins Multiple Vulnerabilities (Apr 2018) - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.637
Fixed version: 2.116
Installation
path / port: /

Impact
Successful exploitation will allow remote attackers to execute a script on victim's Web browser within the security context of the hosting Web site and also disclose sensitive information.

Solution:
Solution type: VendorFix
Update to Jenkins weekly to 2.116 or later, Jenkins LTS to 2.107.2 or later. Please see the references for more information.

Affected Software/OS
Jenkins 2.115 and older, LTS 2.107.1 and older.

Vulnerability Insight
Multiple flaws are due to:
- Some JavaScript confirmation dialogs included the item name in an unsafe manner.
- The Jenkins CLI send different error responses for commands with view and agent arguments depending on the existence of the specified views or agents to unauthorized users.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Jenkins Multiple Vulnerabilities (Apr 2018) - Windows
OID:1.3.6.1.4.1.25623.1.0.813315
Version used: 2021-09-29T12:07:39Z

References
cve: CVE-2018-1000169
cve: CVE-2018-1000170
url: https://jenkins.io/security/advisory/2018-04-11/

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://ip-10-0-0-21.us-east-2.compute.internal:8484/configure:privateKeyPassword`

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.

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: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_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: 4.7)
NVT: Jenkins 'CVE-2017-17383' XSS Vulnerability - Windows

Summary

. . . continues on next page . . .

... continued from previous page ...

Jenkins is prone to an XSS vulnerability.

Vulnerability Detection Result

```
Installed version: 1.637
Fixed version:     See workaround in vendor advisory
Installation
path / port:       /
```

Impact

Successful exploitation would allow an authenticated attacker to expose other users to malicious code.

Solution:

Solution type: Workaround

Please refer to the vendor advisory for a workaround.

Affected Software/OS

Jenkins LTS 2.73.1 and prior, Jenkins 2.93 and prior.

Vulnerability Insight

An authenticated attacker can use a crafted tool name in a job configuration form to conduct XSS attacks.

Vulnerability Detection Method

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

Details: `Jenkins 'CVE-2017-17383' XSS Vulnerability - Windows`

OID:1.3.6.1.4.1.25623.1.0.113064

Version used: `2021-09-16T08:01:42Z`

References

```
cve: CVE-2017-17383
url: https://jenkins.io/security/advisory/2017-12-05/
```

Medium (CVSS: 4.3)

NVT: Jenkins < 2.319.2, < 2.330 CSRF Vulnerability - Windows

Summary

Jenkins is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.637
Fixed version:     2.330
Installation
path / port:       /
```

... continues on next page ...

... continued from previous page ...

Impact
This vulnerability allows attackers to trigger build of job without parameters.

Solution:
Solution type: VendorFix
Update to version 2.330, 2.319.2 LTS or later.

Affected Software/OS
Jenkins version 2.329 and prior and 2.319.1 LTS and prior.

Vulnerability Insight
Jenkins does not require POST requests for the HTTP endpoint handling manual build requests when no security realm is set, resulting in a CSRF vulnerability.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.319.2, < 2.330 CSRF Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.147445
Version used: `2022-01-20T03:03:39Z`

References
`cve: CVE-2022-20612`
`url: https://www.jenkins.io/security/advisory/2022-01-12/`
`cert-bund: WID-SEC-2022-1908`
`dfn-cert: DFN-CERT-2022-0328`
`dfn-cert: DFN-CERT-2022-0086`

Medium (CVSS: 4.3)
NVT: Jenkins < 2.287, < 2.277.2 LTS Multiple Vulnerabilities - Windows

Summary
Jenkins is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.637
Fixed version:     2.287
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 2.287, 2.277.2 LTS or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Jenkins prior to version 2.287, Jenkins LTS prior to version 2.277.2.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-21639: Jenkins does not validate the type of object created after loading the data submitted to the config.xml REST API endpoint of a node.
- CVE-2021-21640: Jenkins does not properly check that a newly created view has an allowed name allowing attackers with View/Create permission to create views with invalid or used names.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Jenkins < 2.287, < 2.277.2 LTS Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.127166
Version used: `2022-09-07T10:10:59Z`

References
`cve: CVE-2021-21639`
`cve: CVE-2021-21640`
`url: https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-1871`
`url: https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-1721`
`dfn-cert: DFN-CERT-2021-1618`
`dfn-cert: DFN-CERT-2021-0711`

[return to 10.0.0.21]

2.1.17 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows

Product detection result
`cpe:/a:openbsd:openssh:7.1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.1
Fixed version:     7.8
Installation
path / port:       22/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

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.

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 < 7.8 User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2023-02-24T10:20:04Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2018-15473`
`url: https://0day.city/cve-2018-15473.html`
`url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d`
`↪1e0`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K18/1031`
`cert-bund: CB-K18/0873`
`dfn-cert: DFN-CERT-2021-2178`
`dfn-cert: DFN-CERT-2020-2189`
`dfn-cert: DFN-CERT-2020-0228`
`dfn-cert: DFN-CERT-2019-2046`
`dfn-cert: DFN-CERT-2019-0857`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2259`
`dfn-cert: DFN-CERT-2018-2191`
`dfn-cert: DFN-CERT-2018-1806`
`dfn-cert: DFN-CERT-2018-1696`

Medium (CVSS: 5.3)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)

Product detection result
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.1
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 Windows

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 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: 2023-07-14T16:09:27Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
cve: CVE-2017-15906
url: https://www.openssh.com/txt/release-7.6

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/101552
url: https://github.com/openbsd/src/commit/a6981567e8e
cert-bund: CB-K20/0041
cert-bund: CB-K18/0137
cert-bund: CB-K17/2126
cert-bund: CB-K17/2014
cert-bund: CB-K17/2002
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2017-2217
dfn-cert: DFN-CERT-2017-2100
dfn-cert: DFN-CERT-2017-2093
```

Medium (CVSS: 5.3)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     None
Installation
path / port:       22/tcp
```

Impact

Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force 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

... continues on next page ...

... continued from previous page ...

OpenSSH version 5.9 through 7.8.

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 - Windows`
OID:1.3.6.1.4.1.25623.1.0.813887
Version used: `2021-05-28T07:06:21Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2018-15919`
`url: https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`url: https://seclists.org/oss-sec/2018/q3/180`
`cert-bund: CB-K18/0885`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2191`

[return to 10.0.0.21]

2.1.18 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result
```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)                | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)              | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
```

... continues on next page ...

... continued from previous page ...

```
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

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

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪------------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

Impact

... continues on next page ...

... continued from previous page ...

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2021-11-15T10:28:20Z`

References
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1112

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 2023-05-13 05:33:38.
Certificate details:

fingerprint (SHA-1)	4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)	AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD5B23381002A885F556
issued by	CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US
public key algorithm	RSA
public key size (bits)	2048
serial	04A9972F
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)	None
valid from	2013-05-15 05:33:38 UTC
valid until	2023-05-13 05:33:38 UTC

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: 2021-11-22T15:32:39Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary

... continues on next page ...

... continued from previous page ...

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

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.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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 the references).
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.

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: `2021-02-12T06:42:15Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.0.0.21]

2.1.19 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: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.21[49154]
     Annotation: Impl friendly name
Port: 49164/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_ip_tcp:10.0.0.21[49164]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49185/tcp
      UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.21[49185]
      UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.21[49185]
      Named pipe : HydraLsPipe
      Win32 service or process : lserver.exe
      Description : Terminal Server Licensing
Port: 49211/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:10.0.0.21[49211]
Port: 49212/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.21[49212]
      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:10.0.0.21[49212]
      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:
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: 2022-06-03T10:17:07Z

[return to 10.0.0.21]

2.1.20 Medium 8585/tcp

Medium (CVSS: 6.8)
NVT: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.4.31
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.4.31, 8.0.24, 8.1.11 or later.

Affected Software/OS
PHP versions prior to 7.4.31, 8.0.x prior to 8.0.24 and 8.1.x prior to 8.1.11.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-31628: The phar uncompressor code would recursively uncompress 'quines' gzip files, resulting in an infinite loop.
- CVE-2022-31629: The vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Windows
OID:1.3.6.1.4.1.25623.1.0.104332
Version used: 2022-09-30T10:11:44Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2022-31628
cve: CVE-2022-31629

... continues on next page ...

... continued from previous page ...

```
url: https://www.php.net/ChangeLog-7.php#7.4.31
url: https://www.php.net/ChangeLog-8.php#8.0.24
url: https://www.php.net/ChangeLog-8.php#8.1.11
url: https://bugs.php.net/bug.php?id=81726
url: https://bugs.php.net/bug.php?id=81727
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-1567
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2023-0422
dfn-cert: DFN-CERT-2022-2869
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2523
dfn-cert: DFN-CERT-2022-2337
dfn-cert: DFN-CERT-2022-2157
```

Medium (CVSS: 6.8)
NVT: PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)

Product detection result

```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to a heap-based use-after-free vulnerability.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     7.1.32
Installation
path / port:       8585/tcp
```

Solution:

Solution type: VendorFix

Update to version 7.1.32 or later.

Affected Software/OS

PHP versions before 7.1.32.

Vulnerability Insight

PHP is prone to a heap use-after-free in pcrelib (cmb).

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108636
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: http://bugs.php.net/75457`
`url: https://www.php.net/ChangeLog-7.php#7.1.32`

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
`Installed Version: 5.3.10`
`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
Update 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:

... continues on next page ...

... continued from previous page ...

- An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script.
- An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.806648
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-7804
cve: CVE-2015-7803
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/76959
url: https://bugs.php.net/bug.php?id=70433
url: http://www.openwall.com/lists/oss-security/2015/10/05/8
cert-bund: CB-K16/0944
cert-bund: CB-K16/0912
cert-bund: CB-K16/0623
cert-bund: CB-K16/0422
cert-bund: CB-K16/0161
cert-bund: CB-K16/0136
cert-bund: CB-K15/1792
cert-bund: CB-K15/1453
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2016-0972
dfn-cert: DFN-CERT-2016-0676
dfn-cert: DFN-CERT-2016-0460
dfn-cert: DFN-CERT-2016-0176
dfn-cert: DFN-CERT-2016-0154
dfn-cert: DFN-CERT-2015-1898
dfn-cert: DFN-CERT-2015-1530

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities - Sep19 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 7.2.22`
`Installation path / port: 8585/tcp`

Solution:
Solution type: VendorFix
Update to version 7.2.22, 7.3.9 or later.

Affected Software/OS
PHP versions before 7.2.22 and 7.3.x before 7.3.9.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Buffer overflow in zendparse
- Cast to object confuses GC, causes crash
- Exif crash (bus error) due to wrong alignment and invalid cast
- Use-after-free in FPM master event handling

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - Sep19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108638
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: http://bugs.php.net/78363`
`url: http://bugs.php.net/78379`
`url: http://bugs.php.net/78333`
`url: http://bugs.php.net/77185`
`url: https://www.php.net/ChangeLog-7.php#7.3.9`
`url: https://www.php.net/ChangeLog-7.php#7.2.22`

Medium (CVSS: 6.8)
NVT: PHP XML Handling Heap Buffer Overflow Vulnerability - Jul13 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a heap based buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.27

Impact
Successful exploitation will allow attackers to cause a heap-based buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.

Solution:
Solution type: VendorFix
Update to PHP version 5.3.27 or later.

Affected Software/OS
PHP version prior to 5.3.27

Vulnerability Insight
The flaw is triggered as user-supplied input is not properly validated when handling malformed XML input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP XML Handling Heap Buffer Overflow Vulnerability - Jul13 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803729
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2013-4113
url: http://php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/61128
url: https://bugs.php.net/bug.php?id=65236

... continues on next page ...

... continued from previous page ...

```
url: http://seclists.org/oss-sec/2013/q3/88
url: http://seclists.org/bugtraq/2013/Jul/106
cert-bund: WID-SEC-2023-1285
cert-bund: CB-K17/1176
cert-bund: CB-K15/0689
cert-bund: CB-K14/0231
cert-bund: CB-K13/0802
dfn-cert: DFN-CERT-2017-1209
dfn-cert: DFN-CERT-2015-0724
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-1450
dfn-cert: DFN-CERT-2013-1446
dfn-cert: DFN-CERT-2013-1445
dfn-cert: DFN-CERT-2013-1444
dfn-cert: DFN-CERT-2013-1392
dfn-cert: DFN-CERT-2013-1347
dfn-cert: DFN-CERT-2013-1331
dfn-cert: DFN-CERT-2013-1316
dfn-cert: DFN-CERT-2013-1315
dfn-cert: DFN-CERT-2013-1299
```

Medium (CVSS: 6.5)
NVT: PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.26
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.26 or later.

Affected Software/OS
PHP versions before 7.2.26.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

PHP is prone to multiple vulnerabilities:
- Buffer underflow in bc_shift_addsub (CVE-2019-11046)
- link() silently truncates after a null byte on Windows (CVE-2019-11044)
- DirectoryIterator class silently truncates after a null byte (CVE-2019-11045)
- Use-after-free in exif parsing under memory sanitizer (CVE-2019-11050)
- Heap-buffer-overflow READ in exif (CVE-2019-11047)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.143277
Version used: `2021-08-30T14:01:20Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2019-11046`
`cve: CVE-2019-11045`
`cve: CVE-2019-11044`
`cve: CVE-2019-11050`
`cve: CVE-2019-11047`
`url: https://www.php.net/ChangeLog-7.php#7.2.26`
`cert-bund: WID-SEC-2022-2122`
`cert-bund: CB-K20/1199`
`cert-bund: CB-K19/1099`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-0550`
`dfn-cert: DFN-CERT-2020-0415`
`dfn-cert: DFN-CERT-2020-0382`
`dfn-cert: DFN-CERT-2020-0339`
`dfn-cert: DFN-CERT-2019-2709`
`dfn-cert: DFN-CERT-2019-2659`

Medium (CVSS: 6.5)
NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Sep 2021) - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

... continues on next page ...

... continued from previous page ...

Summary
PHP released new versions which include a security fix.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.3.31
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.31, 7.4.24, 8.0.11 or later.

Affected Software/OS
PHP versions prior to 7.3.31, 7.4.x through 7.4.23 and 8.0.x through 8.0.10.

Vulnerability Insight
Fixed bug #81420 (ZipArchive::extractTo extracts outside of destination).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Sep 2021) - Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.117695
Version used: 2021-10-25T12:34:47Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21706
url: https://www.php.net/ChangeLog-7.php#7.3.31
url: https://www.php.net/ChangeLog-7.php#7.4.24
url: https://www.php.net/ChangeLog-8.php#8.0.11
url: http://bugs.php.net/81420
cert-bund: WID-SEC-2022-2112
cert-bund: CB-K21/1008
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-1994

Medium (CVSS: 6.5)
NVT: PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 7.1.20`
`Installation path / port: 8585/tcp`

Impact
Successfully exploitation will allow an attacker 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 exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812519
Version used: `2023-01-19T10:10:48Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2015-9253
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
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2022-0455
dfn-cert: DFN-CERT-2022-0431
dfn-cert: DFN-CERT-2020-0337
dfn-cert: DFN-CERT-2018-1882

Medium (CVSS: 6.5)
NVT: WordPress < 5.1 Path Traversal Vulnerability (Windows)

Summary
WordPress allows Path Traversal in wp_crop_image(). An attacker (who has privileges to crop an image) can write the output image to an arbitrary directory via a filename containing two image extensions and ../ sequences, such as a filename ending with the .jpg?/../../file.jpg substring.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 5.1
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to WordPress version 5.1 or later.

Affected Software/OS
WordPress version 5.0.3 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress < 5.1 Path Traversal Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.142031
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2019-8943
url: https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
url: http://www.securityfocus.com/bid/107089
cert-bund: CB-K19/0155

Medium (CVSS: 6.5)
NVT: WordPress Ninja Forms Plugin < 3.5.8 Multiple Vulnerabilities

Summary
The WordPress plugin 'Ninja Forms' is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.5.8
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.5.8 or later.

Affected Software/OS
WordPress Ninja Forms plugin through version 3.5.7.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-34647: Unprotected REST-API to sensitive information disclosure
- CVE-2021-34648: Unprotected REST-API to email injection

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.5.8 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.146888
Version used: `2022-07-20T10:33:02Z`

References
```
cve: CVE-2021-34647
cve: CVE-2021-34648
url: https://www.wordfence.com/blog/2021/09/recently-patched-vulnerabilities-in-
↪ninja-forms-plugin-affects-over-1-million-site-owners/
url: https://wordpress.org/plugins/ninja-forms/#developers
```

Medium (CVSS: 6.5)
NVT: PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Windows)

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

... continues on next page ...

... continued from previous page ...

PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.34
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Affected Software/OS
PHP versions prior 7.2.34, 7.3 prior 7.3.23 and 7.4 prior to 7.4.11.

Vulnerability Insight
The following vulnerabilities exist:
- Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069)
- PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (.
↪..
OID:1.3.6.1.4.1.25623.1.0.144695
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-7069
cve: CVE-2020-7070
url: https://www.php.net/ChangeLog-7.php#7.2.34
url: https://www.php.net/ChangeLog-7.php#7.3.23
url: https://www.php.net/ChangeLog-7.php#7.4.11
cert-bund: WID-SEC-2022-2115
cert-bund: CB-K20/0949
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2021-2373
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-0380

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2187
dfn-cert: DFN-CERT-2020-2111

Medium (CVSS: 6.4)
NVT: PHP EXIF Header Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.4.0 beta 4

Impact
Successful exploitation allows remote attackers to execute arbitrary code, obtain sensitive information or cause a denial of service.

Solution:
Solution type: VendorFix
Update to PHP version 5.4.0 beta 4 or later.

Affected Software/OS
PHP version 5.4.0 beta 2 on Windows.

Vulnerability Insight
The flaw is due to an integer overflow error in 'exif_process_IFD_TAG' function in the 'ext/exif/exif.c' file, Allows remote attackers to cause denial of service via crafted offset_val value in an EXIF header.

Vulnerability Detection Method
Details: PHP EXIF Header Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.802349
Version used: 2021-04-13T14:13:08Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2011-4566
url: https://bugs.php.net/bug.php?id=60150
url: http://olex.openlogic.com/wazi/2011/php-5-4-0-medium/
url: https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4566
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0130
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2012-0070
dfn-cert: DFN-CERT-2012-0003

Medium (CVSS: 6.1)
NVT: WordPress Multiple Vulnerabilities - September19 (Windows)

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.15
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to 5.2.3, 5.1.2, 5.0.6, 4.9.11, 4.8.10, 4.7.14, 4.6.15, 4.5.18, 4.4.19, 4.3.20, 4.2.24, 4.1.27, 4.0.27, 3.9.28, 3.8.30 or 3.7.30 respectively.

Affected Software/OS
WordPress 5.2.x before 5.2.3, 5.1.x before 5.1.2, 5.0.x before 5.0.6, 4.9.x before 4.9.11, 4.8.x before 4.8.10, 4.7.x before 4.7.14, 4.6.x before 4.6.15, 4.5.x before 4.5.18, 4.4.x before 4.4.19, 4.3.x before 4.3.20, 4.2.x before 4.2.24, 4.1.x before 4.1.27, 4.0.x before 4.0.27, 3.9.x before 3.9.28, 3.8.x before 3.8.30 and all previous versions before 3.7.30.

Vulnerability Insight
The following vulnerabilities exist:
- a cross-site scripting (XSS) vulnerability found in post previews by contributors and a cross-site scripting vulnerability in stored comments
- an issue where validation and sanitization of a URL could lead to an open redirect

... continues on next page ...

... continued from previous page ...

- reflected cross-site scripting during media uploads
- a vulnerability for cross-site scripting (XSS) in shortcode previews
- a case where reflected cross-site scripting could be found in the dashboard
- an issue with URL sanitization that can lead to cross-site scripting (XSS) attacks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities - September19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.112639
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2019-16217`
`cve: CVE-2019-16218`
`cve: CVE-2019-16219`
`cve: CVE-2019-16220`
`cve: CVE-2019-16221`
`cve: CVE-2019-16222`
`cve: CVE-2019-16223`
`url: https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/`
`dfn-cert: DFN-CERT-2020-0955`
`dfn-cert: DFN-CERT-2020-0030`
`dfn-cert: DFN-CERT-2019-1850`

Medium (CVSS: 6.1)
NVT: WampServer < 3.1.5 XSS Vulnerability

Summary
WampServer is prone to an XSS vulnerability.

Vulnerability Detection Result
`Installed version: 2.2`
`Fixed version: 3.1.5`

Impact
Successful exploitation would allow an attacker to create a crafted link to inject arbitrary HTML and JavaScript into the target website.

Solution:
Solution type: VendorFix
Update to version 3.1.5.

Affected Software/OS
WampServer before version 3.1.5.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
The script checks if a vulnerable version is present on the target host.
Details: `WampServer < 3.1.5 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112471
Version used: `2021-05-28T07:06:21Z`

References
`cve: CVE-2018-1000848`
`url: http://forum.wampserver.com/read.php?2,153491`

Medium (CVSS: 6.1)
NVT: WordPress Ninja Forms Plugin < 3.2.14 XSS Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
`Installed version: 2.9.42`
`Fixed version: 3.2.14`
`Installation path / port: /wordpress/wp-content/plugins/ninja-forms`

Solution:
Solution type: VendorFix
Update to version 3.2.14 or later.

Affected Software/OS
WordPress Ninja Forms plugin before version 3.2.14.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.2.14 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112239
Version used: `2023-01-17T10:10:58Z`

References
`cve: CVE-2018-7280`
`url: https://wordpress.org/plugins/ninja-forms/#developers`

Medium (CVSS: 6.1)
NVT: WordPress Ninja Forms Plugin < 3.3.18 XSS Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

The WordPress plugin 'Ninja Forms' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 2.9.42
Fixed version:     3.3.18
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.3.18 or later.

Affected Software/OS
WordPress Ninja Forms plugin before version 3.3.18.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.3.18 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112514
Version used: `2023-01-17T10:10:58Z`

References

```
cve: CVE-2018-19287
url: https://wordpress.org/plugins/ninja-forms/#developers
url: https://www.exploit-db.com/exploits/45880
```

Medium (CVSS: 6.1)
NVT: WordPress Ninja Forms Plugin < 3.3.19.1 Open Redirect Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to an open redirect vulnerability.

Vulnerability Detection Result

```
Installed version: 2.9.42
Fixed version:     3.3.19.1
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.3.19.1 or later.

Affected Software/OS
WordPress Ninja Forms plugin before version 3.3.19.1.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The open redirect vulnerability allows remote attackers to redirect a user via the lib/StepProcessing/step-processing.php (aka submissions download page) redirect parameter.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.3.19.1 Open Redirect Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112448
Version used: `2023-01-17T10:10:58Z`

References
`cve: CVE-2018-19796`
`url: https://wordpress.org/plugins/ninja-forms/#developers`

Medium (CVSS: 6.1)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`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
Update 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 Windows

Vulnerability Insight
The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Cross-Site Scripting Vulnerability - Aug16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808799
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-8935
url: https://bugs.php.net/bug.php?id=68978
url: http://www.securityfocus.com/bid/92356
cert-bund: CB-K16/1614
cert-bund: CB-K16/1257
cert-bund: CB-K16/1230
cert-bund: CB-K16/1179
cert-bund: CB-K16/1106
cert-bund: CB-K16/1030
dfn-cert: DFN-CERT-2016-1719
dfn-cert: DFN-CERT-2016-1335
dfn-cert: DFN-CERT-2016-1295
dfn-cert: DFN-CERT-2016-1253
dfn-cert: DFN-CERT-2016-1178
dfn-cert: DFN-CERT-2016-1097

Medium (CVSS: 6.1)
NVT: WordPress Multiple Vulnerabilities Mar17 (Windows)

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.7.3

Impact
Successfully exploiting will allow remote attacker to create a specially crafted URL, execute arbitrary script code in an user's browser session within the trust relationship between their browser and the server and leading to excessive use of server resources.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to WordPress version 4.7.3 or later.

Affected Software/OS
WordPress versions 4.7.2 and prior on Windows.

Vulnerability Insight
Multiple flaws are due to:
- A cross-site scripting (XSS) vulnerability in media file metadata.
- An improper URL validation.
- Unintended files can be deleted by administrators using the plugin deletion functionality.
- A cross-site scripting (XSS) in video URL in YouTube embeds.
- A Cross-site request forgery (CSRF) in Press.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities Mar17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809895
Version used: `2023-03-01T10:20:05Z`

References
```
cve: CVE-2017-6804
cve: CVE-2017-6815
cve: CVE-2017-6814
cve: CVE-2017-6816
cve: CVE-2017-6818
cve: CVE-2017-6817
cve: CVE-2017-6819
url: https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance
↪-release
cert-bund: CB-K17/0387
dfn-cert: DFN-CERT-2017-0395
```

Medium (CVSS: 6.1)
NVT: WordPress Ninja Forms Plugin < 3.4.24.2 CSRF Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.4.24.2
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation would allow an attacker to perform actions in the context of another user.

Solution:
Solution type: VendorFix
Update to version 3.4.24.2.

Affected Software/OS
WordPress Ninja Forms plugin through version 3.4.24.1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.4.24.2 CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113679
Version used: `2023-01-17T10:10:58Z`

References
`cve: CVE-2020-12462`
`url: https://wordpress.org/plugins/ninja-forms/#developers`

Medium (CVSS: 6.1)
NVT: PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     5.6.33
Installation
path / port:       8585/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
Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1

Vulnerability Insight
Multiple flaws are due to:
- An input validation error on the PHAR 404 error page via the URI of a request for a .phar file.
- An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812732
Version used: `2021-08-10T15:24:26Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-5712`
`cve: CVE-2018-5711`
`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`
`cert-bund: CB-K20/0307`
`cert-bund: CB-K18/0498`
`cert-bund: CB-K18/0270`
`cert-bund: CB-K18/0188`
`cert-bund: CB-K18/0174`
`dfn-cert: DFN-CERT-2020-0774`
`dfn-cert: DFN-CERT-2020-0680`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2019-0212`
`dfn-cert: DFN-CERT-2019-0204`
`dfn-cert: DFN-CERT-2018-1739`
`dfn-cert: DFN-CERT-2018-0835`
`dfn-cert: DFN-CERT-2018-0733`
`dfn-cert: DFN-CERT-2018-0576`
`dfn-cert: DFN-CERT-2018-0537`
`dfn-cert: DFN-CERT-2018-0290`
`dfn-cert: DFN-CERT-2018-0205`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-0191

Medium (CVSS: 6.1)
NVT: WordPress Multiple Vulnerabilities (Apr 2018) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.9.5
Installation
path / port: /wordpress

Impact
Successful exploitation will allow remote attackers to conduct cross site scripting, url redirection attacks and bypass security restrictions.

Solution:
Solution type: VendorFix
Update to WordPress version 4.9.5 or later. Please see the references for more information.

Affected Software/OS
WordPress versions prior to 4.9.5.

Vulnerability Insight
Multiple flaws are due to:
- The version string was not escaped in the 'get_the_generator' function.
- The URL validator assumed URLs with the hostname localhost were on the same host as the WordPress server.
- The redirection URL for the login page was not validated or sanitized if forced to use HTTPS.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Multiple Vulnerabilities (Apr 2018) - Windows
OID:1.3.6.1.4.1.25623.1.0.813087
Version used: 2023-03-01T10:20:05Z

References
cve: CVE-2018-10100
cve: CVE-2018-10101
cve: CVE-2018-10102
url: https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance
↪-release
cert-bund: CB-K18/0563
dfn-cert: DFN-CERT-2018-0624

Medium (CVSS: 6.1)
NVT: WordPress Multiple Vulnerabilities (Jan 2018) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.6.1`
`Fixed version: 4.9.2`

Impact
Successful exploitation will allow remote attackers to conduct cross site scripting attacks.

Solution:
Solution type: VendorFix
Update to WordPress version 4.9.2 or later.

Affected Software/OS
WordPress versions prior to 4.9.2.

Vulnerability Insight
An XSS flaw exists in the Flash fallback files in MediaElement, a library that is included with WordPress. Because the Flash files are no longer needed for most use cases, they have been removed from WordPress.
21 other bugs were fixed in WordPress 4.9.2:
- JavaScript errors that prevented saving posts in Firefox have been fixed.
- The previous taxonomy-agnostic behavior of get_category_link() and category_description() was restored.
- Switching themes will now attempt to restore previous widget assignments, even when there are no sidebars to map.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (Jan 2018) - Windows`
OID:1.3.6.1.4.1.25623.1.0.812507
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2018-5776`
`url: https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance`
`↪-release/`
`url: https://codex.wordpress.org/Version_4.9.2`

Medium (CVSS: 5.9)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Windows)

. . . continues on next page . . .

... continued from previous page ...

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
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
Update to PHP version 5.5.28, or 5.6.12, or later.

Affected Software/OS
PHP versions prior to 5.5.28 and 5.6.x before 5.6.12 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Denial of Service Vulnerability - 01 - Jul16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808612
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-8878
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/90837

Medium (CVSS: 5.9)
NVT: WordPress Password Reset CVE-2017-8295 Security Bypass Vulnerability (Windows)

Summary
WordPress is prone to a security-bypass vulnerability.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     None
```

Impact
Attackers can exploit this issue to bypass certain security restrictions to perform unauthorized actions. This may aid in further attacks.

Solution:
Solution type: Workaround
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. A workaround is to enable UseCanonicalName to enforce static SERVER_NAME value.

Affected Software/OS
WordPress versions 4.7.4 and prior.

Vulnerability Insight
The flaws exist because WordPress relies on the Host HTTP header for a password-reset e-mail message, which makes it easier for user-assisted remote attackers to reset arbitrary passwords by making a crafted wp-login.php?action=lostpassword request and then arranging for this e-mail to bounce or be resent, leading to transmission of the reset key to a mailbox on an attacker-controlled SMTP server. This is related to problematic use of the SERVER_NAME variable in wp-includes/pluggable.php in conjunction with the PHP mail function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Password Reset CVE-2017-8295 Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108156
Version used: `2023-03-01T10:20:05Z`

References
```
cve: CVE-2017-8295
url: https://www.exploit-db.com/exploits/41963/
url: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day
↪-CVE-2017-8295.html
url: http://www.securityfocus.com/bid/98295
url: https://httpd.apache.org/docs/2.4/mod/core.html#usecanonicalname
```

Medium (CVSS: 5.8)
NVT: PHP Multiple Vulnerabilities - 01 - Mar13 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.4.0`

Impact
Successful exploitation will allow attackers to retrieve, corrupt or upload arbitrary files, or can cause denial of service via corrupted $_FILES indexes.

Solution:
Solution type: VendorFix
Update to PHP 5.4.0 or later.

Affected Software/OS
PHP version before 5.4.0

Vulnerability Insight
Flaw due to insufficient validation of file-upload implementation in rfc1867.c and it does not handle invalid '[' characters in name values.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - 01 - Mar13 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803341
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2012-1172`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/53403`
`url: http://cxsecurity.com/cveshow/CVE-2012-1172`

... continues on next page ...

... continued from previous page ...

```
url: http://secunia.com/advisories/cve_reference/CVE-2012-1172
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0870
dfn-cert: DFN-CERT-2012-0869
dfn-cert: DFN-CERT-2012-0866
dfn-cert: DFN-CERT-2012-0813
dfn-cert: DFN-CERT-2012-0773
```

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

Summary
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
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213

... continues on next page ...

... continued from previous page ...

Version used: 2022-05-12T09:32:01Z

References

cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.4)
NVT: WampServer 3.1.1 XSS Vulnerability

Summary

WampServer is prone to an XSS vulnerability.

Vulnerability Detection Result

Installed version: 2.2
Fixed version: 3.1.2

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation would allow an attacker to create a crafted link to inject arbitrary HTML and JavaScript into the target website.

Solution:
Solution type: VendorFix
Update to version 3.1.2.

Affected Software/OS
WampServer through version 3.1.1.

Vulnerability Insight
The XSS is possible through the virtual_del parameter.

Vulnerability Detection Method
The script checks if a vulnerable version is present on the target host.
Details: `WampServer 3.1.1 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113139
Version used: `2021-05-28T07:06:21Z`

References
`cve: CVE-2018-8732`
`url: http://forum.wampserver.com/read.php?2,138295,150615,page=6#msg-150615`

Medium (CVSS: 5.4)
NVT: PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     7.2.29
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.2.29 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions before 7.2.29.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Use-of-uninitialized-value in exif (CVE-2020-7064)
- get_headers() silently truncates after a null byte (CVE-2020-7066)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.143616
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2020-7064`
`cve: CVE-2020-7066`
`url: https://www.php.net/ChangeLog-7.php#7.2.29`
`cert-bund: WID-SEC-2022-2118`
`cert-bund: CB-K21/0068`
`cert-bund: CB-K20/1199`
`cert-bund: CB-K20/0239`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-1438`
`dfn-cert: DFN-CERT-2020-1202`
`dfn-cert: DFN-CERT-2020-0965`
`dfn-cert: DFN-CERT-2020-0851`
`dfn-cert: DFN-CERT-2020-0787`
`dfn-cert: DFN-CERT-2020-0554`

Medium (CVSS: 5.4)
NVT: WordPress Ninja Forms Plugin < 3.4.23 XSS Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.4.23
```

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        /wordpress/wp-content/plugins/ninja-forms
```

Impact
Successful exploitation would allow an attacker to inject malicious content into an affected site.

Solution:
Solution type: VendorFix
Update to version 3.4.23 or later.

Affected Software/OS
WordPress Ninja Forms plugin before version 3.4.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.4.23 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112697
Version used: `2023-01-17T10:10:58Z`

References
`cve: CVE-2020-8594`
`url: https://wordpress.org/plugins/ninja-forms/#developers`
`url: https://spider-security.co.uk/blog-cve-cve-2020-8594`

Medium (CVSS: 5.3)
NVT: PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.3.10
Fixed version:     7.2.28
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.2.28 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions before 7.2.28.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062)
- Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-2020-7063)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.143542
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2020-7062`
`cve: CVE-2020-7063`
`url: https://www.php.net/ChangeLog-7.php#7.2.28`
`cert-bund: WID-SEC-2022-2119`
`cert-bund: CB-K20/0147`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-1438`
`dfn-cert: DFN-CERT-2020-0787`
`dfn-cert: DFN-CERT-2020-0518`
`dfn-cert: DFN-CERT-2020-0485`
`dfn-cert: DFN-CERT-2020-0341`

Medium (CVSS: 5.3)
NVT: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.3.29
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.29 or later.

Affected Software/OS
PHP versions prior to 7.3.29.

Vulnerability Insight
The following flaws exist:
- CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL.
- CVE-2021-21704: Stack buffer overflow in firebird_info_cb.
- CVE-2021-21704: SIGSEGV in firebird_handle_doer.
- CVE-2021-21704: SIGSEGV in firebird_stmt_execute.
- CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Windows
OID:1.3.6.1.4.1.25623.1.0.117525
Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21704
cve: CVE-2021-21705
url: https://www.php.net/ChangeLog-7.php#7.3.29
url: http://bugs.php.net/81122
url: http://bugs.php.net/76448
url: http://bugs.php.net/76449
url: http://bugs.php.net/76450
url: http://bugs.php.net/76452
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-1577
cert-bund: WID-SEC-2022-0624

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K21/0705
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-1046
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1676
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-1627
dfn-cert: DFN-CERT-2021-1509
dfn-cert: DFN-CERT-2021-1453
dfn-cert: DFN-CERT-2021-1419

Medium (CVSS: 5.3)
NVT: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP released new versions which include a security fix.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.3.33
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.33, 7.4.26, 8.0.13 or later.

Affected Software/OS
PHP prior to version 7.3.33 and version 7.4.x through 7.4.25 and 8.0.x through 8.0.12.

Vulnerability Insight
Fixed bug #79971 (special character is breaking the path in xml function).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.147188

... continues on next page ...

... continued from previous page ...

Version used: 2021-12-02T03:03:37Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21707
url: https://www.php.net/ChangeLog-7.php#7.3.33
url: https://www.php.net/ChangeLog-7.php#7.4.26
url: https://www.php.net/ChangeLog-8.php#8.0.13
url: http://bugs.php.net/79971
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0587
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1213
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2869
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2499
dfn-cert: DFN-CERT-2022-1516
dfn-cert: DFN-CERT-2022-1493
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2022-0455
dfn-cert: DFN-CERT-2022-0431
dfn-cert: DFN-CERT-2022-0407
dfn-cert: DFN-CERT-2022-0110
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-2436

Medium (CVSS: 5.3)
NVT: PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

... continues on next page ...

... continued from previous page ...

PHP is prone to two Denial-of-Service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.2.31
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Affected Software/OS
PHP versions prior 7.2.31, 7.3 prior 7.3.18 and 7.4 prior to 7.4.6.

Vulnerability Insight
The following flaws exist:
- Long filenames cause OOM and temp files to not be cleaned
- Long variables in multipart/form-data cause OOM and temp files are not cleaned
leading to a Denial-of-Service condition (CVE-2019-11048).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (W.
↪..
OID:1.3.6.1.4.1.25623.1.0.143914
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2019-11048
url: https://www.php.net/ChangeLog-7.php#7.2.31
url: https://www.php.net/ChangeLog-7.php#7.3.18
url: https://www.php.net/ChangeLog-7.php#7.4.6
url: https://bugs.php.net/bug.php?id=78875
url: https://bugs.php.net/bug.php?id=78876
cert-bund: WID-SEC-2022-2117
cert-bund: CB-K20/1199
cert-bund: CB-K20/0467
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2020-2627

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1964
dfn-cert: DFN-CERT-2020-1438
dfn-cert: DFN-CERT-2020-1376
dfn-cert: DFN-CERT-2020-1202
dfn-cert: DFN-CERT-2020-1019

Medium (CVSS: 5.3)
NVT: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.3.26
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Affected Software/OS
PHP versions prior to 7.3.26, 7.4.x prior to 7.4.14 and 8.0.x prior to 8.0.1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - W.
↪..
OID:1.3.6.1.4.1.25623.1.0.145115
Version used: 2021-11-29T15:00:35Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2020-7071
url: https://www.php.net/ChangeLog-7.php#7.3.26
url: https://www.php.net/ChangeLog-7.php#7.4.14
url: https://www.php.net/ChangeLog-8.php#8.0.1
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-2114
cert-bund: CB-K21/0009
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2021-2373
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-1509
dfn-cert: DFN-CERT-2021-1453
dfn-cert: DFN-CERT-2021-0380
dfn-cert: DFN-CERT-2021-0013

Medium (CVSS: 5.3)
NVT: WordPress Ninja Forms Plugin < 3.4.28 Missing Escaping Vulnerability

Summary
The WordPress plugin 'Ninja Forms' lacks escaping for submissions-table fields.

Vulnerability Detection Result
Installed version: 2.9.42
Fixed version: 3.4.28
Installation
path / port: /wordpress/wp-content/plugins/ninja-forms

Solution:
Solution type: VendorFix
Update to version 3.4.28 or later.

Affected Software/OS
WordPress Ninja Forms plugin version 3.4.27.1 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Ninja Forms Plugin < 3.4.28 Missing Escaping Vulnerability
OID:1.3.6.1.4.1.25623.1.0.145243
Version used: 2023-01-17T10:10:58Z

References
cve: CVE-2020-36173
url: https://wordpress.org/plugins/ninja-forms/#developers

Medium (CVSS: 5.3)
NVT: WordPress Ninja Forms Plugin < 3.4.27.1 Multiple Vulnerabilities

Summary
The WordPress plugin 'Ninja Forms' is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.4.27.1
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.4.27.1 or later.

Affected Software/OS
WordPress Ninja Forms plugin version 3.4.27 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CSRF via services integration (CVE-2020-36174)
- Validation bypass via the email field (CVE-2020-36175)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.4.27.1 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.145242
Version used: `2023-01-17T10:10:58Z`

References
```
cve: CVE-2020-36174
cve: CVE-2020-36175
url: https://wordpress.org/plugins/ninja-forms/#developers
```

Medium (CVSS: 5.3)
NVT: WordPress <= 4.7.2 Path Disclosure Vulnerability

Summary
WordPress is prone to a path disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     4.7.3
Installation
path / port:       /wordpress
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation would allow an attacker to access sensitive information.

Solution:
Solution type: VendorFix
Update to version 4.7.3 or above.

Affected Software/OS
WordPress through version 4.7.2.

Vulnerability Insight
The vulnerability exists because WordPress mishandles the listings of post authors, which allows remote attackers to obtain sensitive information via a /wp-json/oembed/1.0/embed?url= request, related to the 'author_name:' substring.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress <= 4.7.2 Path Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113415
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2017-6514`
`url: https://web.archive.org/web/20180612235401/https://github.com/CFSECURITE/wo`
`↪rdpress`
`url: http://www.securityfocus.com/bid/108459`

Medium (CVSS: 5.2)
NVT: WordPress Ninja Forms Plugin < 3.6.13 Insecure Deserialization Vulnerability

Summary
The WordPress plugin Ninja Forms is prone to an insecure deseralization vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.6.13
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.6.13 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress Ninja Forms plugin prior to version 3.6.13.

Vulnerability Insight
The plugin unserialises the content of an imported file, which could lead to PHP object injections issues when an admin import a malicious file and a suitable gadget chain is present on the blog.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.6.13 Insecure Deserialization Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.126158
Version used: `2022-09-29T10:24:47Z`

References
`cve: CVE-2022-2903`
`url: https://wpscan.com/vulnerability/255b98ba-5da9-4424-a7e9-c438d8905864`

Medium (CVSS: 5.1)
NVT: PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a heap-based buffer overflow vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.3.29`

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
PHP versions 5.6.x 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 Windows

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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 (Windows)
OID:1.3.6.1.4.1.25623.1.0.809742
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2014-4049
url: http://php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/68007
url: http://www.openwall.com/lists/oss-security/2014/06/13/4
cert-bund: CB-K16/0944
cert-bund: CB-K15/0493
cert-bund: CB-K14/1359
cert-bund: CB-K14/1174
cert-bund: CB-K14/1167
cert-bund: CB-K14/1110
cert-bund: CB-K14/0973
cert-bund: CB-K14/0972
cert-bund: CB-K14/0834
cert-bund: CB-K14/0830
cert-bund: CB-K14/0829
cert-bund: CB-K14/0805
cert-bund: CB-K14/0776
cert-bund: CB-K14/0750
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2014-1434
dfn-cert: DFN-CERT-2014-1219
dfn-cert: DFN-CERT-2014-1166
dfn-cert: DFN-CERT-2014-1014
dfn-cert: DFN-CERT-2014-1013
dfn-cert: DFN-CERT-2014-0870
dfn-cert: DFN-CERT-2014-0868
dfn-cert: DFN-CERT-2014-0867
dfn-cert: DFN-CERT-2014-0839
dfn-cert: DFN-CERT-2014-0816
dfn-cert: DFN-CERT-2014-0782

Medium (CVSS: 5.0)
NVT: PHP 'open_basedir' Secuirity Bypass Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.15

Impact
Successful exploitation could allow attackers to bypass certain security restrictions.

Solution:
Solution type: VendorFix
Update to PHP 5.3.15 or later.

Affected Software/OS
PHP version before 5.3.15

Vulnerability Insight
Flaw in SQLite functionality allows attackers to bypass the open_basedir protection mechanism.

Vulnerability Detection Method
Details: PHP 'open_basedir' Secuirity Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803318
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-3365
url: http://www.php.net/ChangeLog-5.php
url: http://www.securityfocus.com/bid/54612
url: http://en.securitylab.ru/nvd/427459.php
url: http://secunia.com/advisories/cve_reference/CVE-2012-3365
cert-bund: CB-K17/1176
dfn-cert: DFN-CERT-2017-1209

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1655
dfn-cert: DFN-CERT-2012-1654
dfn-cert: DFN-CERT-2012-1541
dfn-cert: DFN-CERT-2012-1422

Medium (CVSS: 5.0)
NVT: WordPress / WordPress MU Multiple Vulnerabilities - July09

Summary
WordPress / WordPress MU is prone to multiple vulnerabilities

Vulnerability Detection Result
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8585/wordpress/wp-settings.php

Impact
Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information.

Solution:
Solution type: VendorFix
Update to Version 2.8.1 or later.

Affected Software/OS
WordPress / WordPress MU version prior to 2.8.1.

Vulnerability Insight
- Error in 'wp-settings.php' which may disclose sensitive information via a direct request.
- Error occur when user attempt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames.
- Error in wp-admin/admin.php is does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details: WordPress / WordPress MU Multiple Vulnerabilities - July09
OID:1.3.6.1.4.1.25623.1.0.800662
Version used: 2023-03-01T10:20:04Z

References
cve: CVE-2009-2432
cve: CVE-2009-2336
cve: CVE-2009-2335

... continues on next page ...

... continued from previous page ...

cve: CVE-2009-2334
url: http://www.vupen.com/english/advisories/2009/1833
url: http://www.securityfocus.com/bid/35581
url: http://www.securityfocus.com/bid/35584
url: http://securitytracker.com/alerts/2009/Jul/1022528.html
url: http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded
dfn-cert: DFN-CERT-2010-0125
dfn-cert: DFN-CERT-2009-1593
dfn-cert: DFN-CERT-2009-1208
dfn-cert: DFN-CERT-2009-1188
dfn-cert: DFN-CERT-2009-1144
dfn-cert: DFN-CERT-2009-1081

Medium (CVSS: 5.0)
NVT: WordPress Unspecified Vulnerability (May 2023) - Windows

Summary
WordPress is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 5.9.7
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 5.9.7, 6.0.5, 6.1.3, 6.2.2 or later.
Note: 5.8.x and previous branches appear to have not received a fix. According to the advisory, the vendor may not provide a fix:
'All versions since WordPress 5.9 have also been updated.'

Affected Software/OS
WordPress version 6.2.1 and prior.

Vulnerability Insight
The update block themes parsing shortcodes in user-generated data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Unspecified Vulnerability (May 2023) - Windows
OID:1.3.6.1.4.1.25623.1.0.104757
Version used: 2023-05-24T09:09:06Z

References
url: https://wordpress.org/news/2023/05/wordpress-6-2-2-security-release/

Medium (CVSS: 5.0)
NVT: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 8.0.29
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 8.0.29, 8.1.10, 8.2.7 or later.

Affected Software/OS
PHP prior to version 8.0.29, 8.1.x prior to 8.1.20 and 8.2.x prior to 8.2.7.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Windows
OID:1.3.6.1.4.1.25623.1.0.149761
Version used: 2023-06-21T05:06:23Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2023-3247
url: https://www.php.net/ChangeLog-8.php#8.0.29
url: https://www.php.net/ChangeLog-8.php#8.1.20
url: https://www.php.net/ChangeLog-8.php#8.2.7
url: https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw
cert-bund: WID-SEC-2023-1506
dfn-cert: DFN-CERT-2023-1328

Medium (CVSS: 5.0)
NVT: PHP 'openssl_encrypt()' Function Information Disclosure Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to an information disclosure vulnerability.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.3.14`

Impact
Successful exploitation will allow remote attackers to obtain sensitive information from process memory by providing zero bytes of input data.

Solution:
Solution type: VendorFix
Apply the patch or upgrade to the latest version from the references.

Affected Software/OS
PHP version 5.3.9 through 5.3.13 on Windows

Vulnerability Insight
The flaw is due to error in 'openssl_encrypt()' function when handling empty $data strings which will allow an attacker to gain access to arbitrary pieces of information in current memory.

Vulnerability Detection Method
Details: `PHP 'openssl_encrypt()' Function Information Disclosure Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803164
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2012-6113`
`url: https://bugs.php.net/bug.php?id=61413`
`url: http://www.securityfocus.com/bid/57462`
`url: http://xforce.iss.net/xforce/xfdb/81400`
`url: http://git.php.net/?p=php-src.git;a=commitdiff;h=270a406ac94b5fc5cc9ef59fc6`

... continues on next page ...

... continued from previous page ...

↪1e3b4b95648a3e

Medium (CVSS: 5.0)
NVT: Apache HTTP Server mod_proxy_ajp Process Timeout DoS Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.2.22
Installation
path / port: 8585/tcp

Impact
Successful exploitation could allow remote attackers to cause a denial of service condition via an expensive request.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.22 or later.

Affected Software/OS
Apache HTTP Server version 2.2.12 through 2.2.21.

Vulnerability Insight
The flaw is due to an error in the mod_proxy_ajp module, which places a worker node into an error state upon detection of a long request-processing time.

Vulnerability Detection Method
Details: Apache HTTP Server mod_proxy_ajp Process Timeout DoS Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.802683
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2012-4557
url: https://bugzilla.redhat.com/show_bug.cgi?id=871685
url: http://www.securityfocus.com/bid/56753
url: http://httpd.apache.org/security/vulnerabilities_22.html#2.2.22
url: http://svn.apache.org/viewvc?view=revision&revision=1227298
dfn-cert: DFN-CERT-2013-0342
dfn-cert: DFN-CERT-2013-0237
dfn-cert: DFN-CERT-2012-2191

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.4.55
Installation
path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.55 or later.

Affected Software/OS
Apache HTTP Server version 2.4.54 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2006-20001: mod_dav out of bounds read, or write of zero byte
- CVE-2022-36760: Possible request smuggling in mod_proxy_ajp
- CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.149153

... continues on next page ...

... continued from previous page ...

Version used: 2023-01-18T10:11:02Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2006-20001
cve: CVE-2022-36760
cve: CVE-2022-37436
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0110
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0548
dfn-cert: DFN-CERT-2023-0497
dfn-cert: DFN-CERT-2023-0118

Medium (CVSS: 5.0)
NVT: WordPress Multiple Vulnerabilities - July09

Summary
WordPress is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8585/wordpress/wp
↪-settings.php

Impact
Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information.

Solution:
Solution type: VendorFix
Update to Version 2.8.1 or later.

Affected Software/OS
WordPress version prior to 2.8.1 on all running platform.

Vulnerability Insight
- Error in 'wp-settings.php' which may disclose the sensitive information via a direct request.

... continues on next page ...

... continued from previous page ...

- username of a post's author is placed in an HTML comment, which allows remote attackers to obtain sensitive information by reading the HTML source.
- Error occur when user attempt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames.
- wp-admin/admin.php does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details: WordPress Multiple Vulnerabilities - July09
OID:1.3.6.1.4.1.25623.1.0.800657
Version used: 2023-03-01T10:20:04Z

References
cve: CVE-2009-2432
cve: CVE-2009-2431
cve: CVE-2009-2336
cve: CVE-2009-2335
cve: CVE-2009-2334
url: http://www.vupen.com/english/advisories/2009/1833
url: http://www.securityfocus.com/bid/35581
url: http://www.securityfocus.com/bid/35584
url: http://securitytracker.com/alerts/2009/Jul/1022528.html
url: http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded
dfn-cert: DFN-CERT-2010-0125
dfn-cert: DFN-CERT-2009-1593
dfn-cert: DFN-CERT-2009-1208
dfn-cert: DFN-CERT-2009-1188
dfn-cert: DFN-CERT-2009-1144
dfn-cert: DFN-CERT-2009-1081

Medium (CVSS: 5.0)
NVT: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Windows

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an IMAP header injection vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 7.3.28
Installation

... continues on next page ...

... continued from previous page ...

path / port: 8585/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.28, 7.4.18 or later.

Affected Software/OS
PHP versions prior to 7.3.28 and 7.4.x through 7.4.17.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - W.
↪..
OID:1.3.6.1.4.1.25623.1.0.145870
Version used: 2021-05-03T08:21:47Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
url: https://www.php.net/ChangeLog-7.php#7.3.28
url: https://www.php.net/ChangeLog-7.php#7.4.18

Medium (CVSS: 5.0)
NVT: WordPress Multiple Vulnerabilities (May 2023) - Windows

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.6.1
Fixed version: 4.6.26
Installation
path / port: /wordpress

Solution:
Solution type: VendorFix
Update to version 4.1.38, 4.2.35, 4.3.31, 4.4.30, 4.5.29, 4.6.26, 4.7.26, 4.8.22, 4.9.23, 5.0.19, 5.1.16, 5.2.18, 5.3.15, 5.4.13, 5.5.12, 5.6.11, 5.7.9, 5.8.7, 5.9.6, 6.0.4, 6.1.2, 6.2.1 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

WordPress version 6.2.0 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- No CVE: Block themes parsing shortcodes in user generated data
- No CVE: A CSRF issue updating attachment thumbnails
- No CVE: A flaw allowing XSS via open embed auto discovery
- No CVE: Bypassing of KSES sanitization in block attributes for low privileged users
- CVE-2023-2745: A path traversal issue via translation files

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities (May 2023) - Windows`
OID:1.3.6.1.4.1.25623.1.0.104753
Version used: `2023-05-22T12:17:59Z`

References
```
cve: CVE-2023-2745
url: https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-rel
↪ease/
url: https://www.wordfence.com/blog/2023/05/wordpress-core-6-2-1-security-mainte
↪nance-release-what-you-need-to-know/
url: https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordp
↪ress-core-621-directory-traversal
cert-bund: WID-SEC-2023-1231
dfn-cert: DFN-CERT-2023-1137
```

Medium (CVSS: 5.0)
NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Windows

Product detection result
```
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP released new versions which include security fixes.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     7.3.30
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.3.30, 7.4.23, 8.0.10 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions prior to 7.3.30, 7.4.x through 7.4.22 and 8.0.x through 8.0.9.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Windo.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.146585
Version used: `2021-10-25T12:34:47Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: https://www.php.net/ChangeLog-7.php#7.3.30`
`url: https://www.php.net/ChangeLog-7.php#7.4.23`
`url: https://www.php.net/ChangeLog-8.php#8.0.10`

Medium (CVSS: 5.0)
NVT: PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Windows

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     7.4.33
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.4.33, 8.0.25, 8.1.12 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP prior to version 7.4.33, version 8.0.x through 8.0.24 and 8.1.x through 8.1.11.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-31630: OOB read due to insufficient input validation in imageloadfont()
- CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Windows`
OID:1.3.6.1.4.1.25623.1.0.148831
Version used: `2022-11-04T10:11:50Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2022-31630`
`cve: CVE-2022-37454`
`url: https://www.php.net/ChangeLog-7.php#7.4.33`
`url: https://www.php.net/ChangeLog-8.php#8.0.25`
`url: https://www.php.net/ChangeLog-8.php#8.1.12`
`cert-bund: WID-SEC-2023-1021`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0138`
`cert-bund: WID-SEC-2022-1934`
`cert-bund: WID-SEC-2022-1816`
`dfn-cert: DFN-CERT-2023-0552`
`dfn-cert: DFN-CERT-2023-0422`
`dfn-cert: DFN-CERT-2023-0028`
`dfn-cert: DFN-CERT-2022-2869`
`dfn-cert: DFN-CERT-2022-2793`
`dfn-cert: DFN-CERT-2022-2715`
`dfn-cert: DFN-CERT-2022-2639`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2022-2598`
`dfn-cert: DFN-CERT-2022-2535`
`dfn-cert: DFN-CERT-2022-2523`
`dfn-cert: DFN-CERT-2022-2420`
`dfn-cert: DFN-CERT-2022-2380`

Medium (CVSS: 5.0)
NVT: PHP Multiple Vulnerabilities - Jun13 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.3.10`
`Fixed version: 5.3.26/5.4.16`

Impact
Successful exploitation allows attackers to execute arbitrary code or cause denial of service condition via crafted arguments.

Solution:
Solution type: VendorFix
Update to PHP 5.4.16 or 5.3.26 or later.

Affected Software/OS
PHP version before 5.3.26 and 5.4.x before 5.4.16

Vulnerability Insight
Multiple flaws are due to:
- Heap-based overflow in 'php_quot_print_encode' function in 'ext/standard/quot_print.c' script.
- Integer overflow in the 'SdnToJewish' function in 'jewish.c' in the Calendar component.

Vulnerability Detection Method
Details: `PHP Multiple Vulnerabilities - Jun13 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803678
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2013-4635`
`cve: CVE-2013-2110`
`url: http://www.php.net/ChangeLog-5.php`

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/60411
url: http://www.securityfocus.com/bid/60731
url: http://bugs.php.net/bug.php?id=64895
url: http://bugs.php.net/bug.php?id=64879
url: http://www.security-database.com/detail.php?alert=CVE-2013-4635
url: http://www.security-database.com/detail.php?alert=CVE-2013-2110
cert-bund: CB-K14/1480
dfn-cert: DFN-CERT-2014-1566
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-1450
dfn-cert: DFN-CERT-2013-1446
dfn-cert: DFN-CERT-2013-1445
dfn-cert: DFN-CERT-2013-1444
dfn-cert: DFN-CERT-2013-1392
dfn-cert: DFN-CERT-2013-1347
dfn-cert: DFN-CERT-2013-1195

Medium (CVSS: 4.8)
NVT: WordPress Ninja Forms Plugin <= 3.6.9 XSS Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to a stored cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 2.9.42
Fixed version: 3.6.10
Installation
path / port: /wordpress/wp-content/plugins/ninja-forms

Solution:
Solution type: VendorFix
Update to version 3.6.10 or later.

Affected Software/OS
WordPress Ninja Forms plugin version 3.6.9 and prior.

Vulnerability Insight
Authenticated attackers (admin or higher user role) can conduct a stored XSS attack via 'lable'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Ninja Forms Plugin <= 3.6.9 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.124085
Version used: 2022-07-20T10:33:02Z

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-36827
url: https://patchstack.com/database/vulnerability/ninja-forms/wordpress-ninja-f
↪orms-contact-form-plugin-3-6-9-authenticated-stored-cross-site-scripting-xss-v
↪ulnerability

Medium (CVSS: 4.8)
NVT: WordPress Ninja Forms Contact Form Plugin < 3.6.10 Multiple Vulnerabilities

Summary
The WordPress plugin 'Ninja Forms Contact Form' is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.9.42
Fixed version: 3.6.10
Installation
path / port: /wordpress/wp-content/plugins/ninja-forms

Solution:
Solution type: VendorFix
Update to version 3.6.10 or later.

Affected Software/OS
WordPress Ninja Forms Contact Form plugin prior to version 3.6.10.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-25056: The plugin does not sanitise and escape field labels, allowing high privilege users to perform cross-site scripting attacks even when the unfiltered_html capability is disallowed.
- CVE-2021-25066:The plugin does not sanitize and escape some imported data, allowing high privilege users to perform cross-site scripting attacks even when the unfiltered_html capability is disallowed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Ninja Forms Contact Form Plugin < 3.6.10 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.127070
Version used: 2022-07-20T10:33:02Z

References
cve: CVE-2021-25056
cve: CVE-2021-25066
url: https://wpscan.com/vulnerability/795acab2-f621-4662-834b-ebb6205ef7de
url: https://wpscan.com/vulnerability/323d5fd0-abe8-44ef-9127-eea6fd4f3f3d

Medium (CVSS: 4.8)
NVT: WordPress Ninja Forms Plugin < 3.5.8.2 XSS Vulnerability

Summary
The WordPress plugin 'Ninja Forms' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.5.8.2
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.5.8.2 or later.

Affected Software/OS
WordPress Ninja Forms plugin through version 3.5.8.1.

Vulnerability Insight
The plugin does not sanitise and escape the custom class name of the form field created, which could allow high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Plugin < 3.5.8.2 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147081
Version used: `2022-07-20T10:33:02Z`

References
```
cve: CVE-2021-24381
url: https://wpscan.com/vulnerability/e383fae6-e0da-4aba-bb62-adf51c01bf8d
url: https://wordpress.org/plugins/ninja-forms/#developers
```

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://ip-10-0-0-21.us-east-2.compute.internal:8585/wordpress/wp-login.php?redir
↪ect_to=http%3A%2F%2Fip-10-0-0-21.us-east-2.compute.internal%3A8585%2Fwordpress
```

... continues on next page ...

... continued from previous page ...

↪%2Fwp-admin%2F&reauth=1:pwd

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.

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: 2020-08-24T15:18:35Z

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_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: 4.7)
NVT: PHP Security Bypass Vulnerability May18 (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a security bypass vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.3.10
Fixed version:     5.6.35
Installation
path / port:       8585/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
Update 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 Windows.

Vulnerability Insight
The flaw exists as the dumpable FPM child processes allow bypassing opcache access controls

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Security Bypass Vulnerability May18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813161
Version used: `2021-06-03T02:00:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-10545`
`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`
`cert-bund: CB-K18/0633`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2018-1232`
`dfn-cert: DFN-CERT-2018-0920`
`dfn-cert: DFN-CERT-2018-0877`

Medium (CVSS: 4.6)
NVT: Apache HTTP Server Scoreboard Security Bypass Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 2.2.21
Fixed version: 2.2.22
Installation
path / port: 8585/tcp

Impact
Successful exploitation will allow remote attacker to bypass certain security restrictions. Other attacks are also possible.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.22 or later.

Affected Software/OS
Apache HTTP Server version before 2.2.22.

Vulnerability Insight
The flaw is due to an error in 'inscoreboard.c', certain type field within a scoreboard shared memory segment leading to an invalid call to the free function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Scoreboard Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803744
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2012-0031

. . . continues on next page . . .

... continued from previous page ...

```
url: http://svn.apache.org/viewvc?view=revision&revision=1230065
url: http://www.securityfocus.com/bid/51407
url: http://www.halfdog.net/Security/2011/ApacheScoreboardInvalidFreeOnShutdown
cert-bund: CB-K14/1505
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0740
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

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

Product detection result
`cpe:/a:apache:http_server:2.2.21`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

Summary
Apache HTTP Server is prone to a 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.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
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.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188

Medium (CVSS: 4.3)
NVT: PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.4.18/5.5.2

Impact
Successful exploitation will allow remote attackers to spoof the server via a MitM (Man-in-the-Middle) attack and disclose potentially sensitive information.

Solution:
Solution type: VendorFix
Update to PHP version 5.4.18 or 5.5.2 or later.

Affected Software/OS
PHP versions before 5.4.18 and 5.5.x before 5.5.2 on Windows.

Vulnerability Insight
The flaw is due to the SSL module not properly handling NULL bytes inside 'subjectAltNames' general names in the server SSL certificate.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803739
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2013-4248
url: http://secunia.com/advisories/54480
url: http://www.securityfocus.com/bid/61776
url: http://www.php.net/ChangeLog-5.php

... continues on next page ...

... continued from previous page ...

```
url: http://git.php.net/?p=php-src.git;a=commit;h=2874696a5a8d46639d261571f915c4
↪93cd875897
cert-bund: WID-SEC-2023-1284
cert-bund: CB-K14/0834
cert-bund: CB-K14/0231
cert-bund: CB-K13/1092
cert-bund: CB-K13/0712
cert-bund: CB-K13/0609
dfn-cert: DFN-CERT-2014-0870
dfn-cert: DFN-CERT-2013-2127
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1603
dfn-cert: DFN-CERT-2013-1538
dfn-cert: DFN-CERT-2013-1537
```

Medium (CVSS: 4.3)
NVT: PHP 'main/SAPI.c' HTTP Header Injection Vulnerability

Product detection result
cpe:/a:php:php:5.3.10
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an HTTP header injection vulnerability.

Vulnerability Detection Result
Installed version: 5.3.10
Fixed version: 5.3.11/5.4.1 RC1

Impact
Successful exploitation could allows remote attackers to insert arbitrary headers, conduct cross-site request-forgery, cross-site scripting, HTML-injection, and other attacks.

Solution:
Solution type: VendorFix
Update to PHP 5.4.1 RC1 or later.

Affected Software/OS
PHP version prior to 5.3.11, PHP version 5.4.x through 5.4.0RC2 on Windows

Vulnerability Insight
The sapi_header_op function in main/SAPI.c in PHP does not properly determine a pointer during checks for %0D sequences.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: PHP 'main/SAPI.c' HTTP Header Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.802966
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-4388
cve: CVE-2011-1398
url: http://openwall.com/lists/oss-security/2012/09/02/1
url: http://www.securityfocus.com/bid/55297
url: http://www.securityfocus.com/bid/55527
url: http://openwall.com/lists/oss-security/2012/09/07/3
url: http://article.gmane.org/gmane.comp.php.devel/70584
url: http://openwall.com/lists/oss-security/2012/09/05/15
url: http://security-tracker.debian.org/tracker/CVE-2012-4388
cert-bund: CB-K13/1037
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2013-2065
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-1444
dfn-cert: DFN-CERT-2013-0357
dfn-cert: DFN-CERT-2012-1840
dfn-cert: DFN-CERT-2012-1789
dfn-cert: DFN-CERT-2012-1775
dfn-cert: DFN-CERT-2012-1772

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'mod_dav_svn' Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.2.21
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.2.21

... continues on next page ...

... continued from previous page ...

Fixed version: 2.2.25
Installation
path / port: 8585/tcp

Impact
Successful exploitation will allow remote attacker to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.25 or later.

Affected Software/OS
Apache HTTP Server version before 2.2.25.

Vulnerability Insight
The flaw is due to an error in 'mod_dav.c', It does not properly determine whether DAV is enabled for a URI.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 'mod_dav_svn' Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803743
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.21
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2013-1896
url: http://www.apache.org/dist/httpd/Announcement2.2.html
url: http://www.securityfocus.com/bid/61129
url: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/mod_dav.c?v
↪iew=log
cert-bund: CB-K15/0960
cert-bund: CB-K14/1568
cert-bund: CB-K14/1095
cert-bund: CB-K14/0231
cert-bund: CB-K13/1009
cert-bund: CB-K13/0600
dfn-cert: DFN-CERT-2015-1008
dfn-cert: DFN-CERT-2014-1668
dfn-cert: DFN-CERT-2014-1145

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2013-2027
dfn-cert: DFN-CERT-2013-1587
dfn-cert: DFN-CERT-2013-1503
dfn-cert: DFN-CERT-2013-1464
dfn-cert: DFN-CERT-2013-1463
dfn-cert: DFN-CERT-2013-1456
```

[return to 10.0.0.21]

2.1.21 Medium 3920/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: 2021-11-22T15:32:39Z

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 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)              | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)            | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                        | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 04A9972F
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)  | None
valid from                       | 2013-05-15 05:33:38 UTC
valid until                      | 2023-05-13 05:33:38 UTC
```

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: 2021-11-22T15:32:39Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

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.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
```

. . . continues on next page . . .

... continued from previous page ...

```
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

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 the references).
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.

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: 2021-02-12T06:42:15Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 10.0.0.21]

2.1.22 Medium 8020/tcp

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8020/WEB-INF../we
↪b.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
```

... continues on next page ...

... continued from previous page ...

```
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- Caucho Resin version 2.1.12 on Apache HTTP server version 1.3.29
Other products and versions might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/WEB-INF../web.xml
http://example.com/web-inf../web.xml
(note the double dot ('..') after 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INF../' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117221
Version used: `2023-06-16T05:06:18Z`

References
`cve: CVE-2004-0281`
`url: http://marc.info/?l=bugtraq&m=107635084830547&w=2`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/9617
```

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

Summary
Various application or web servers / products are prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:8020/WEB-INf./web
↪.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
```

... continues on next page ...

... continued from previous page ...

```
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

Impact
Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.

Solution:
Solution type: VendorFix
Please contact the vendor for more information on possible fixes.

Affected Software/OS
The following products are known to be affected:
- A misconfigured reverse proxy.
Other products might be affected as well.

Vulnerability Insight
The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.
This means that URLs like:
http://example.com/WEB-INF/web.xml
will return an error message, rather than the contents of the deployment descriptor.
However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:
http://example.com/META-INf./web.xml
(note the 'f.' in 'WEB-INF').

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INf./' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117225
Version used: `2023-03-06T10:19:58Z`

References
`url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667`

[return to 10.0.0.21]

2.1.23 Medium 3389/tcp

Medium (CVSS: 5.0)
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_RC4_128_MD5
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:
- 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: 2021-12-01T13:10:37Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

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.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
```

... continues on next page ...

... continued from previous page ...

```
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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=metasploitable3-win2k8
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)
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

... continues on next page ...

... continued from previous page ...

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: 2021-10-15T11:13:32Z

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

[return to 10.0.0.21]

2.1.24 Medium 9200/tcp

Medium (CVSS: 6.8)
NVT: Elastisearch Remote Code Execution Vulnerability

Summary
Elasticsearch is prone to a remote-code-execution vulnerability.

Vulnerability Detection Result
Vulnerable URL: http://ip-10-0-0-21.us-east-2.compute.internal:9200/_search?source=%7B%22size%22%3A1%2C%22query%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%7D%7D%2C%22script_fields%22%3A%7B%22VTTest%22%3A%7B%22script%22%3A%22import%20java.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2Fwindows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D%7D%7D&callback=?

Impact
An attacker can exploit this issue to execute arbitrary code

Solution:
Solution type: VendorFix
Ask the vendor for an update or disable 'dynamic scripting'

Affected Software/OS
Elasticsearch < 1.2

Vulnerability Insight
Elasticsearch has a flaw in its default configuration which makes it possible for any webpage to execute arbitrary code on visitors with Elasticsearch installed.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: Elastisearch Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105032

... continues on next page ...

... continued from previous page ...

Version used: 2022-12-05T10:11:03Z

References
cve: CVE-2014-3120
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://bouk.co/blog/elasticsearch-rce/
cert-bund: CB-K14/1131
dfn-cert: DFN-CERT-2014-1188

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

Summary
Elasticsearch is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 6.8.17
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 6.8.17, 7.13.3 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.17 and 7.x prior to 7.13.3.

Vulnerability Insight
An uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)
OID:1.3.6.1.4.1.25623.1.0.146386
Version used: 2021-08-17T12:00:57Z

References
cve: CVE-2021-22144
url: https://discuss.elastic.co/t/elasticsearch-7-13-3-and-6-8-17-security-updat
↪e/278100
cert-bund: WID-SEC-2022-1777
dfn-cert: DFN-CERT-2022-2315

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability (Windows)

Summary
Elasticsearch is prone to a field disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.12
Installation
path / port:       /
```

Impact
An attacker could gain additional permissions against a restricted index.

Solution:
Solution type: VendorFix
Update to version 6.8.12, 7.9.1 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.12 and 7.9.0.

Vulnerability Insight
A field disclosure flaw was found in Elasticsearch when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.144431
Version used: `2021-07-07T11:00:41Z`

References
```
cve: CVE-2020-7019
url: https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update
↪/245456
```

Medium (CVSS: 5.9)
NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) (Windows)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.2
Installation
path / port:       /
```

Impact

On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

Solution:

Solution type: VendorFix

Update to version 6.8.2 or 7.2.1 respectively.

Affected Software/OS

Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.

Vulnerability Insight

A race condition flaw was found in the response headers Elasticsearch returns to a request.

Vulnerability Detection Method

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

Details: `Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability. ↪..`

OID:1.3.6.1.4.1.25623.1.0.117162

Version used: `2023-03-06T10:19:58Z`

References

```
cve: CVE-2019-7614
url: https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/
↪192963
url: https://www.elastic.co/community/security/
```

Medium (CVSS: 5.3)

NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)

Summary

Elasticsearch is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     6.8.15
Installation
path / port:       /
```

... continues on next page ...

... continued from previous page ...

Impact
This could lead to disclosing the existence of documents and fields the attacker should not be able to view or result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.15, 7.12.0 or later.

Affected Software/OS
Elasticsearch versions prior to versions 6.8.15 or 7.12.0.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-22135: Suggester & Profile API information disclosure flaw
- CVE-2021-22137: Field disclosure flaw

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)`
OID:1.3.6.1.4.1.25623.1.0.145940
Version used: `2021-08-17T12:00:57Z`

References
`cve: CVE-2021-22135`
`cve: CVE-2021-22137`
`url: https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updat`
`↪e/268125`
`cert-bund: WID-SEC-2022-0720`

Medium (CVSS: 4.9)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.14
Installation
path / port:       /
```

Impact
This could allow an Elasticsearch administrator to view sensitive details.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to version 6.8.14, 7.10.0 or later.

Affected Software/OS
Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.

Vulnerability Insight
Elasticsearch has an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)`
OID:1.3.6.1.4.1.25623.1.0.145383
Version used: `2021-08-17T12:00:57Z`

References
`cve: CVE-2020-7021`
`url: https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-updat`
`↪e/263915`
`url: https://www.elastic.co/community/security`

Medium (CVSS: 4.3)
NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)

Summary
Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
`Installed version: 1.1.1`
`Fixed version: 1.4.0.Beta1`

Impact
Successful exploitation will allow remote attackers to inject arbitrary web script or HTML.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.4.0.Beta1, or later.

Affected Software/OS
Elasticsearch version 1.3.x and prior on Windows.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Flaw is due to an error in the CORS functionality.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808092
Version used: `2022-04-13T13:17:10Z`

References
`cve: CVE-2014-6439`
`url: https://www.elastic.co/community/security/`
`url: http://www.securityfocus.com/bid/70233`
`url: http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded`

[return to 10.0.0.21]

2.1.25 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: MySQL Server Components Multiple Unspecified Vulnerabilities

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20-log`
`Fixed version: See advisory`

Impact
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL version 5.1.x before 5.1.62 and 5.5.x before 5.5.22.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple unspecified errors exist in the Server Optimizer and Server DML components.

Vulnerability Detection Method
Details: MySQL Server Components Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.803808
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-1690
cve: CVE-2012-1688
cve: CVE-2012-1703
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53058
url: http://www.securityfocus.com/bid/53067
url: http://www.securityfocus.com/bid/53074
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1170
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0936
dfn-cert: DFN-CERT-2012-0933
dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.28

... continues on next page ...

... continued from previous page ...

Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.66, 5.5.28 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.65 and prior and 5.5 through 5.5.27.

Vulnerability Insight
The flaw allows remote authenticated users to affect availability, related to GIS Extension.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117201
Version used: 2021-02-12T11:09:59Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-5060
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
dfn-cert: DFN-CERT-2013-0079

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server Multiple Vulnerabilities-02 Nov12 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the references or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.65 and Oracle MySQL version 5.5.x to 5.5.27 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component related to server installation and server optimizer.

Vulnerability Detection Method
Details: Oracle MySQL Server Multiple Vulnerabilities-02 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803112
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-3180
cve: CVE-2012-3177
cve: CVE-2012-3160
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56003
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56027
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.67, 5.5.29 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117203
Version used: 2021-02-12T11:09:59Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-5611
cve: CVE-2013-0384
cve: CVE-2013-0389
cve: CVE-2013-0385
cve: CVE-2013-0375
cve: CVE-2012-1702
cve: CVE-2013-0383
cve: CVE-2012-0572

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2012-0574
cve: CVE-2012-1705
cve: CVE-2012-4414
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
cert-bund: CB-K13/0919
cert-bund: CB-K13/0603
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1597
dfn-cert: DFN-CERT-2013-0259
dfn-cert: DFN-CERT-2013-0192
dfn-cert: DFN-CERT-2013-0119
dfn-cert: DFN-CERT-2013-0118
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2013-0079
dfn-cert: DFN-CERT-2013-0037
dfn-cert: DFN-CERT-2013-0028
dfn-cert: DFN-CERT-2012-2285
dfn-cert: DFN-CERT-2012-2258
dfn-cert: DFN-CERT-2012-2215
dfn-cert: DFN-CERT-2012-2200
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.24
Installation
path / port:       3306/tcp
```

Impact

The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'InnoDB' package / privilege.

Solution:

Solution type: VendorFix

Update to version 5.5.24 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Oracle MySQL Server 5.5.x through 5.5.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows
OID:1.3.6.1.4.1.25623.1.0.117267
Version used: 2021-03-18T11:53:07Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-1735
cve: CVE-2012-1757
cve: CVE-2012-1756
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-1389

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.5.29 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.28.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117205
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2012-5612`
`cve: CVE-2013-0386`
`cve: CVE-2013-0368`
`cve: CVE-2013-0371`
`cve: CVE-2012-0578`
`cve: CVE-2013-0367`
`cve: CVE-2012-5096`
`url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL`
`advisory-id: cpujan2013`
`dfn-cert: DFN-CERT-2013-0259`
`dfn-cert: DFN-CERT-2013-0079`

Medium (CVSS: 6.6)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version:  Apply the patch`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote attackers to have impact on availability, confidentiality and integrity.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier, 5.7.17 and earlier on Windows

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in the 'Server: DML', 'Server: Optimizer', 'Server: Thread Pooling', 'Client mysqldump', 'Server: Security: Privileges' components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows
OID:1.3.6.1.4.1.25623.1.0.810882
Version used: 2022-07-20T10:33:02Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2017-3309
cve: CVE-2017-3308
cve: CVE-2017-3329
cve: CVE-2017-3456
cve: CVE-2017-3453
cve: CVE-2017-3600
cve: CVE-2017-3462
cve: CVE-2017-3463
cve: CVE-2017-3461
cve: CVE-2017-3464
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97742
url: http://www.securityfocus.com/bid/97725
url: http://www.securityfocus.com/bid/97763
url: http://www.securityfocus.com/bid/97831

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/97776
url: http://www.securityfocus.com/bid/97765
url: http://www.securityfocus.com/bid/97851
url: http://www.securityfocus.com/bid/97849
url: http://www.securityfocus.com/bid/97812
url: http://www.securityfocus.com/bid/97818
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1563
cert-bund: CB-K17/1401
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0927
cert-bund: CB-K17/0657
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1630
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0675
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.36 and earlier and 5.6.16 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Performance Schema, Options, RBR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804575
Version used: `2022-07-21T10:11:30Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-2430`
`cve: CVE-2014-2431`
`cve: CVE-2014-2436`
`cve: CVE-2014-2440`
`url: http://secunia.com/advisories/57940`
`url: http://www.securityfocus.com/bid/66850`
`url: http://www.securityfocus.com/bid/66858`
`url: http://www.securityfocus.com/bid/66890`
`url: http://www.securityfocus.com/bid/66896`
`url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638`
`url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0464`
`cert-bund: CB-K14/0452`
`dfn-cert: DFN-CERT-2014-0742`
`dfn-cert: DFN-CERT-2014-0477`
`dfn-cert: DFN-CERT-2014-0459`

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple denial-of-service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows

Vulnerability Insight
Multiple flaws exist due to:
- An error in the 'Server: DDL' component.
- Multiple errors in the 'Server: Optimizer' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows
OID:1.3.6.1.4.1.25623.1.0.812646
Version used: 2022-07-20T10:33:02Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2018-2668
cve: CVE-2018-2665
cve: CVE-2018-2622
cve: CVE-2018-2640
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0480
cert-bund: CB-K18/0392
cert-bund: CB-K18/0265
cert-bund: CB-K18/0096
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0424
dfn-cert: DFN-CERT-2018-0286
dfn-cert: DFN-CERT-2018-0101

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.37 and earlier and 5.6.17 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to SRINFOSC and SRCHAR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.804722
Version used: 2022-04-14T11:24:11Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2014-4258
cve: CVE-2014-4260
url: http://secunia.com/advisories/59521
url: http://www.securityfocus.com/bid/68564
url: http://www.securityfocus.com/bid/68573
url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi
↪ty_patches
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A
↪ppendixMSQL
cert-bund: CB-K15/0567
cert-bund: CB-K14/1420
cert-bund: CB-K14/0891
cert-bund: CB-K14/0868
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2014-1500
dfn-cert: DFN-CERT-2014-0930
dfn-cert: DFN-CERT-2014-0911

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation of this vulnerability will allow remote attackers to compromise availability of the system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.11 and earlier on Windows.

Vulnerability Insight
The flaw exists due to an error in 'Server: Optimizer'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811986
Version used: `2022-07-21T10:11:30Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2017-10378`
`url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html`
`url: http://www.securityfocus.com/bid/101375`
`cert-bund: CB-K18/0480`
`cert-bund: CB-K18/0242`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/2048`
`cert-bund: CB-K17/1748`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-1265`
`dfn-cert: DFN-CERT-2018-0515`
`dfn-cert: DFN-CERT-2018-0260`
`dfn-cert: DFN-CERT-2018-0242`
`dfn-cert: DFN-CERT-2017-2137`
`dfn-cert: DFN-CERT-2017-1827`

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote to compromise availability confidentiality, and integrity of the system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.19 and earlier on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- An error in 'Client programs' component.
- An error in 'Server: DDL'.
- An error in 'Server: Replication'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.811991
Version used: 2023-07-14T16:09:27Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2017-10379
cve: CVE-2017-10384
cve: CVE-2017-10268
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101415
url: http://www.securityfocus.com/bid/101406
url: http://www.securityfocus.com/bid/101390
cert-bund: CB-K18/0480
cert-bund: CB-K18/0242
cert-bund: CB-K18/0224
cert-bund: CB-K17/2048
cert-bund: CB-K17/1748
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0260
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-2137
dfn-cert: DFN-CERT-2017-1827

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (cpuoct2020) - Windows

Product detection result

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.5.20
Fixed version: 5.6.50
Installation
path / port: 3306/tcp

Solution:

Solution type: VendorFix
Update to version 5.6.50, 5.7.32, 8.0.22 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server versions 5.6.49 and prior, 5.7 through 5.7.31 and 8.0 through 8.0.21.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108959
Version used: `2021-08-16T12:00:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2020-14765`
`cve: CVE-2020-14769`
`cve: CVE-2020-14812`
`cve: CVE-2020-14793`
`cve: CVE-2020-14672`
`cve: CVE-2020-14867`
`url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL`
`advisory-id: cpuoct2020`
`cert-bund: CB-K20/1066`
`cert-bund: CB-K20/1017`
`dfn-cert: DFN-CERT-2021-2155`
`dfn-cert: DFN-CERT-2021-0002`
`dfn-cert: DFN-CERT-2020-2763`
`dfn-cert: DFN-CERT-2020-2756`
`dfn-cert: DFN-CERT-2020-2620`
`dfn-cert: DFN-CERT-2020-2380`
`dfn-cert: DFN-CERT-2020-2295`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to an unspecified denial of service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.5.20
Fixed version:     5.6.47
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.47 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.46 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.143359
Version used: `2021-08-16T09:00:57Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2020-2579`
`url: https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL`
`advisory-id: cpujan2020`
`cert-bund: CB-K20/0038`
`dfn-cert: DFN-CERT-2020-1827`
`dfn-cert: DFN-CERT-2020-1078`
`dfn-cert: DFN-CERT-2020-0096`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (cpuoct2019) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.46
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.46, 5.7.28, 8.0.18 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.45 and prior, 5.7 through 5.7.27 and 8.0 through 8.0.17.

Vulnerability Insight
Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.143030
Version used: 2021-09-07T14:01:38Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-2974
cve: CVE-2019-2911
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K20/1030
cert-bund: CB-K20/0109
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2020-2763
dfn-cert: DFN-CERT-2020-2756
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-0658

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2019-2695
dfn-cert: DFN-CERT-2019-2687
dfn-cert: DFN-CERT-2019-2656
dfn-cert: DFN-CERT-2019-2301
dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.51 and prior.

Vulnerability Insight
The flaw exists due to an unspecified error within the 'Server:DML' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809378
Version used: 2022-07-21T10:11:30Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-5624
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K16/1846
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (cpuoct2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server versions 5.5.50 and prior, 5.6 through 5.6.31 and 5.7 through 5.7.13.

Vulnerability Insight
The flaw exists due to an unspecified error in the 'Server: DML' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809374
Version used: `2022-07-21T10:11:30Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-5612`
`url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL`
`advisory-id: cpuoct2016`
`cert-bund: CB-K16/1979`
`cert-bund: CB-K16/1755`
`cert-bund: CB-K16/1742`
`cert-bund: CB-K16/1714`
`cert-bund: CB-K16/1624`
`dfn-cert: DFN-CERT-2016-2089`
`dfn-cert: DFN-CERT-2016-1859`
`dfn-cert: DFN-CERT-2016-1849`
`dfn-cert: DFN-CERT-2016-1790`
`dfn-cert: DFN-CERT-2016-1714`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (cpujul2016) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.49 and prior, 5.6 through 5.6.30 and 5.7 through 5.7.12.

Vulnerability Insight
Multiple unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808588
Version used: `2022-04-13T13:17:10Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-3477`
`cve: CVE-2016-3521`
`cve: CVE-2016-3615`
`cve: CVE-2016-5440`
`url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/91902`
`url: http://www.securityfocus.com/bid/91932`
`url: http://www.securityfocus.com/bid/91960`
`url: http://www.securityfocus.com/bid/91953`
`advisory-id: cpujul2016`
`cert-bund: CB-K16/1755`
`cert-bund: CB-K16/1742`
`cert-bund: CB-K16/1448`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1146
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1540
dfn-cert: DFN-CERT-2016-1217
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.67, 5.5.29 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.803459
Version used: 2022-07-21T10:11:30Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-1531
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.68, 5.5.30, 5.6.11 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.67 and prior, 5.5 through 5.5.29 and 5.6 through 5.6.10.

Vulnerability Insight
Unspecified error in some unknown vectors related to Information Schema.

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

... continues on next page ...

... continued from previous page ...

Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.117206
Version used: 2022-07-21T10:11:30Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-2378
cve: CVE-2013-1506
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59188
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.69, 5.5.31, 5.6.11 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Oracle MySQL Server versions 5.1.68 and prior, 5.5 through 5.5.30 and 5.6 through 5.6.10.

Vulnerability Insight
Unspecified error in Server Optimizer, Server Privileges, InnoDB, and in some unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117207
Version used: `2022-07-21T10:11:30Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-2375`
`cve: CVE-2013-1544`
`cve: CVE-2013-1532`
`cve: CVE-2013-2389`
`cve: CVE-2013-2392`
`cve: CVE-2013-2391`
`url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/59207`
`url: http://www.securityfocus.com/bid/59209`
`url: http://www.securityfocus.com/bid/59224`
`url: http://www.securityfocus.com/bid/59242`
`advisory-id: cpuapr2013`
`dfn-cert: DFN-CERT-2013-0882`
`dfn-cert: DFN-CERT-2013-0839`
`dfn-cert: DFN-CERT-2013-0798`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.68, 5.5.30 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.67 and prior and 5.5 through 5.5.29.

Vulnerability Insight
Unspecified error in Server Partition and in some unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117209
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-1521
cve: CVE-2013-1552
cve: CVE-2013-1555
cve: CVE-2012-5614
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59196
url: http://www.securityfocus.com/bid/59210
advisory-id: cpuapr2013

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.31 and prior and 5.6 through 5.6.11.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.806878
Version used: 2022-09-12T10:18:03Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2016-0502
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81136
advisory-id: cpujan2016
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0104
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:

Solution type: VendorFix

Update to version 5.5.39, 5.6.20 or later.

Affected Software/OS

Oracle MySQL Server versions 5.5.38 and prior and 5.6 through 5.6.19.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Unspecified errors in the MySQL Server component via unknown vectors related to CLIENT:MYSQLADMIN, CLIENT:MYSQLDUMP, SERVER:MEMORY STORAGE ENGINE, SERVER:SSL:yaSSL, SERVER:DML, SERVER:SSL:yaSSL, SERVER:REPLICATION ROW FORMAT BINARY LOG DML, SERVER:CHARACTER SETS, and SERVER:MyISAM.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804782
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-6530`
`cve: CVE-2012-5615`
`cve: CVE-2014-6495`
`cve: CVE-2014-6478`
`cve: CVE-2014-4274`
`cve: CVE-2014-4287`
`cve: CVE-2014-6484`
`cve: CVE-2014-6505`
`cve: CVE-2014-6463`
`cve: CVE-2014-6551`
`url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL`
`advisory-id: cpuoct2014`
`cert-bund: CB-K15/1518`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K15/0415`
`cert-bund: CB-K14/1482`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/1412`
`cert-bund: CB-K14/1299`
`dfn-cert: DFN-CERT-2015-1604`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2015-0427`
`dfn-cert: DFN-CERT-2014-1567`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-1489`
`dfn-cert: DFN-CERT-2014-1357`
`dfn-cert: DFN-CERT-2013-0259`

Medium (CVSS: 6.4)
NVT: Oracle MySQL Server Multiple Vulnerabilities-04 Nov12 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data, and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced vendor advisory or upgrade to the latest version.

Affected Software/OS
Oracle MySQL version 5.5.x to 5.5.26 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component vectors related to MySQL client and server.

Vulnerability Detection Method
Details: Oracle MySQL Server Multiple Vulnerabilities-04 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803114
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-3147
cve: CVE-2012-3149
cve: CVE-2012-3144
url: http://secunia.com/advisories/51008/

. . . continues on next page . . .

... continued from previous page ...

url: http://www.securityfocus.com/bid/56006
url: http://www.securityfocus.com/bid/56008
url: http://www.securityfocus.com/bid/56022
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937

Medium (CVSS: 6.2)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpuoct2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a local unauthenticated vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.45
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight
Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.143032
Version used: 2021-09-08T08:01:40Z

... continues on next page ...

. . . continued from previous page . . .

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-2969
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 6.1)
NVT: Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (cpuapr2016v3) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.47 and prior, 5.6 through 5.6.28 and 5.7 through 5.7.10.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807928
Version used: `2021-10-13T11:01:26Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-0649`
`cve: CVE-2016-0650`
`cve: CVE-2016-0644`
`cve: CVE-2016-0646`
`cve: CVE-2016-0640`
`cve: CVE-2016-0641`
`url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL`
`advisory-id: cpuapr2016v3`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0750`
`cert-bund: CB-K16/0646`
`cert-bund: CB-K16/0597`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0903`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0803`
`dfn-cert: DFN-CERT-2016-0695`
`dfn-cert: DFN-CERT-2016-0644`

Medium (CVSS: 6.1)
NVT: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.41
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.41 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows
OID:1.3.6.1.4.1.25623.1.0.149168
Version used: 2023-01-20T10:11:50Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2023-21840
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL
advisory-id: cpujan2023
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0126
dfn-cert: DFN-CERT-2023-0105

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpuapr2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.43
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.43, 5.7.25, 8.0.14 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

Vulnerability Insight
Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (...
OID:1.3.6.1.4.1.25623.1.0.142405
Version used: 2021-09-07T14:01:38Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2018-3123
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
advisory-id: cpuapr2019
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K19/0319
dfn-cert: DFN-CERT-2019-0775

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a vulnerability in a third party library.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
The flaw makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

Vulnerability Insight
wolfSSL (formerly CyaSSL) as used in MySQL does not properly handle faults associated with the Chinese Remainder Theorem (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117194
Version used: 2022-08-31T10:10:28Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

... continued from previous page ...

References

```
cve: CVE-2015-7744
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
advisory-id: cpujan2016
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0104
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Backronym Vulnerability June16 (Windows)

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to the backronym vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.3
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack.

Solution:

Solution type: VendorFix

Upgrade to version Oracle MySQL Server 5.7.3 or later.

Affected Software/OS

Oracle MySQL Server 5.7.2 and earlier on Windows.

Vulnerability Insight

The flaw exists due to improper validation of MySQL client library when establishing a secure connection to a MySQL server using the –ssl option.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Backronym Vulnerability June16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.808063
Version used: 2022-08-08T10:24:51Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-3152
url: http://www.ocert.org/advisories/ocert-2015-003.html
url: https://duo.com/blog/backronym-mysql-vulnerability
cert-bund: CB-K18/0871
cert-bund: CB-K16/0944
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/1020
cert-bund: CB-K15/0994
cert-bund: CB-K15/0964
cert-bund: CB-K15/0895
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
dfn-cert: DFN-CERT-2015-1051
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0942

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.33
Installation

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.32 and prior and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145794
Version used: 2021-08-26T13:01:12Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2020-1971
cve: CVE-2021-2178
cve: CVE-2021-2202
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0067
cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-2047
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1000
cert-bund: WID-SEC-2022-0585
cert-bund: CB-K21/1065
cert-bund: CB-K21/0788
cert-bund: CB-K21/0615
cert-bund: CB-K21/0421
cert-bund: CB-K21/0111
cert-bund: CB-K21/0062
cert-bund: CB-K21/0006
cert-bund: CB-K20/1217
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2190

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-0924
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2021-0255
dfn-cert: DFN-CERT-2021-0134
dfn-cert: DFN-CERT-2021-0131
dfn-cert: DFN-CERT-2021-0128
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2021-0078
dfn-cert: DFN-CERT-2021-0012
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.35
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.35, 8.0.26 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Oracle MySQL Server version 5.7.34 and prior and 8.0 through 8.0.25.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.146355
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2021-22901`
`cve: CVE-2019-17543`
`cve: CVE-2021-2389`
`cve: CVE-2021-2390`
`cve: CVE-2021-2356`
`cve: CVE-2021-2385`
`cve: CVE-2021-2342`
`cve: CVE-2021-2372`
`cve: CVE-2021-22897`
`cve: CVE-2021-22898`
`url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL`
`advisory-id: cpujul2021`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-0063`
`cert-bund: WID-SEC-2022-1963`
`cert-bund: WID-SEC-2022-0873`
`cert-bund: CB-K22/0044`
`cert-bund: CB-K21/0813`
`cert-bund: CB-K21/0770`
`dfn-cert: DFN-CERT-2022-1892`
`dfn-cert: DFN-CERT-2022-1692`
`dfn-cert: DFN-CERT-2022-1597`
`dfn-cert: DFN-CERT-2022-1241`
`dfn-cert: DFN-CERT-2022-0933`
`dfn-cert: DFN-CERT-2022-0872`
`dfn-cert: DFN-CERT-2022-0666`
`dfn-cert: DFN-CERT-2022-0076`
`dfn-cert: DFN-CERT-2022-0074`
`dfn-cert: DFN-CERT-2021-2527`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2369
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-1743
dfn-cert: DFN-CERT-2021-1677
dfn-cert: DFN-CERT-2021-1593
dfn-cert: DFN-CERT-2021-1580
dfn-cert: DFN-CERT-2021-1537
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-1174
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-1157
dfn-cert: DFN-CERT-2021-1151
dfn-cert: DFN-CERT-2021-1148
dfn-cert: DFN-CERT-2021-1045
dfn-cert: DFN-CERT-2019-2216
```

Medium (CVSS: 5.9)
NVT: Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

Apply the latest patch from vendor. Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL version 5.5.59 and earlier, 5.6.39 and earlier, 5.7.21 and earlier on Windows

Vulnerability Insight
Multiple flaws exist due to
- Multiple errors in the 'Client programs' component of MySQL Server.
- An error in the 'Server: Locking' component of MySQL Server.
- An error in the 'Server: Optimizer' component of MySQL Server.
- Multiple errors in the 'Server: DDL' component of MySQL Server.
- Multiple errors in the 'Server: Replication' component of MySQL Server.
- An error in the 'InnoDB' component of MySQL Server.
- An error in the 'Server : Security : Privileges' component of MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.813148
Version used: `2022-08-08T10:24:51Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2018-2761`
`cve: CVE-2018-2771`
`cve: CVE-2018-2781`
`cve: CVE-2018-2773`
`cve: CVE-2018-2817`
`cve: CVE-2018-2813`
`cve: CVE-2018-2755`
`cve: CVE-2018-2819`
`cve: CVE-2018-2818`
`url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: CB-K18/0608`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-1265`
`dfn-cert: DFN-CERT-2018-0913`
`dfn-cert: DFN-CERT-2018-0723`

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (cpuapr2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.44
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.44, 5.7.26, 8.0.16 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.43 and prior, 5.7 through 5.7.25 and 8.0 through 8.0.15.

Vulnerability Insight
The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.142403
Version used: 2022-03-28T03:06:01Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-1559
cve: CVE-2019-2683

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2019-2627
cve: CVE-2019-2614
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
advisory-id: cpuapr2019
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0462
cert-bund: CB-K22/0045
cert-bund: CB-K20/0041
cert-bund: CB-K19/0911
cert-bund: CB-K19/0639
cert-bund: CB-K19/0623
cert-bund: CB-K19/0622
cert-bund: CB-K19/0620
cert-bund: CB-K19/0619
cert-bund: CB-K19/0615
cert-bund: CB-K19/0332
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0173
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-0092
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2625
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2274
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0968
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412

Medium (CVSS: 5.7)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

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

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Server : Optimizer, DDL, Server : Compiling, Server : Federated.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805172
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-2571
cve: CVE-2015-0505
cve: CVE-2015-0501
cve: CVE-2015-0499
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74095
url: http://www.securityfocus.com/bid/74112
url: http://www.securityfocus.com/bid/74070
url: http://www.securityfocus.com/bid/74115
cert-bund: CB-K15/1546
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551

Medium (CVSS: 5.6)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation of this vulnerability will allow remote to have an impact on availability, confidentiality and integrity.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.53 and earlier, 5.6.34 and earlier, 5.7.16 and earlier on Windows

Vulnerability Insight
Multiple flaws exist due to: multiple unspecified errors in sub components 'Error Handling', 'Logging', 'MyISAM', 'Packaging', 'Optimizer', 'DML' and 'DDL'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.809865
Version used: `2023-07-14T16:09:27Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
cve: CVE-2017-3238
cve: CVE-2017-3318
cve: CVE-2017-3291
cve: CVE-2017-3317
cve: CVE-2017-3258
cve: CVE-2017-3312
cve: CVE-2017-3313
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2017-3244
cve: CVE-2017-3265
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95571
url: http://www.securityfocus.com/bid/95560
url: http://www.securityfocus.com/bid/95491
url: http://www.securityfocus.com/bid/95527
url: http://www.securityfocus.com/bid/95565
url: http://www.securityfocus.com/bid/95588
url: http://www.securityfocus.com/bid/95501
url: http://www.securityfocus.com/bid/95585
url: http://www.securityfocus.com/bid/95520
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/0927
cert-bund: CB-K17/0423
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0430
dfn-cert: DFN-CERT-2017-0090

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow local users to affect availability.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior.

Vulnerability Insight
Unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Optimizer'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows`
OID:1.3.6.1.4.1.25623.1.0.807922
Version used: `2022-08-31T10:10:28Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-0651`
`url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL`
`advisory-id: cpuapr2016v3`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0597`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0644`

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpujul2019) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.45
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight
Oracle MySQL Server is prone to multiple denial of service vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.142645
Version used: 2023-01-31T10:08:41Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-2805
cve: CVE-2019-2740
cve: CVE-2019-2819
cve: CVE-2019-2739
cve: CVE-2019-2737
cve: CVE-2019-2738
url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
advisory-id: cpujul2019
cert-bund: CB-K19/0620
dfn-cert: DFN-CERT-2020-2620

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-0658
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2019-2695
dfn-cert: DFN-CERT-2019-2656
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1568
dfn-cert: DFN-CERT-2019-1453

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.37
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.147465
Version used: 2022-01-26T03:03:43Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log

... continues on next page ...

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

cve: CVE-2021-22946
cve: CVE-2022-21367
cve: CVE-2022-21270
cve: CVE-2022-21304
cve: CVE-2022-21344
cve: CVE-2022-21303
cve: CVE-2022-21245
cve: CVE-2021-22947
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL
advisory-id: cpujan2022
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: CB-K22/0316
cert-bund: CB-K22/0077
cert-bund: CB-K22/0062
cert-bund: CB-K22/0030
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0052
dfn-cert: DFN-CERT-2021-2527

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1931

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation of this vulnerability will allow remote attackers to partially access data, partially modify data, and partially deny service.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, on Windows

Vulnerability Insight
The flaw exists due to an error in the Client programs component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows
OID:1.3.6.1.4.1.25623.1.0.811434
Version used: 2023-07-14T16:09:27Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-3636
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
↪#AppendixMSQL
url: http://www.securityfocus.com/bid/99736
cert-bund: CB-K18/0224
cert-bund: CB-K17/1870
cert-bund: CB-K17/1604
cert-bund: CB-K17/1453
cert-bund: CB-K17/1401
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243
```

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.40
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.40, 8.0.31 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.30.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118388
Version used: 2022-10-24T10:14:58Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-2097
cve: CVE-2022-21617
cve: CVE-2022-21608
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1777
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1146
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1065
cert-bund: WID-SEC-2022-0561
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1058
dfn-cert: DFN-CERT-2023-0509
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2315
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1536
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1515
dfn-cert: DFN-CERT-2022-1497

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.46
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.46, 5.7.28 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.45 and prior and 5.7 through 5.7.27.

Vulnerability Insight
Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.143034
Version used: 2021-09-08T08:01:40Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-2922
cve: CVE-2019-2923
cve: CVE-2019-2924
cve: CVE-2019-2910

. . . continues on next page . . .

... continued from previous page ...

url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack. This may lead to other attacks also.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier on Windows

Vulnerability Insight
The flaw exists due to an incorrect implementation or enforcement of 'ssl-mode=REQUIRED' in MySQL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows
OID:1.3.6.1.4.1.25623.1.0.810884
Version used: 2022-04-13T11:57:07Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2017-3305
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97023
cert-bund: CB-K17/1604
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.47
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.47, 5.7.27 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.46 and prior and 5.7 through 5.7.26.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Wi.

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.143735
Version used: 2021-08-16T09:00:57Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2019-1547
cve: CVE-2019-1549
cve: CVE-2019-1552
cve: CVE-2019-1563
url: https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL
advisory-id: cpuapr2020
cert-bund: WID-SEC-2023-1762
cert-bund: WID-SEC-2023-1049
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/1016
cert-bund: CB-K20/0321
cert-bund: CB-K20/0318
cert-bund: CB-K20/0043
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
cert-bund: CB-K20/0028
cert-bund: CB-K19/1025
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0808
cert-bund: CB-K19/0675
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1900
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1559

Medium (CVSS: 5.0)
NVT: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.5.30 and earlier and 5.6.10 on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Prepared Statements, Server Options and Server Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803725
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2013-3801
cve: CVE-2013-3805
cve: CVE-2013-3794
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61222
url: http://www.securityfocus.com/bid/61256
url: http://www.securityfocus.com/bid/61269
cert-bund: CB-K13/0919
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 5.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)

Product detection result

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact

Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

Solution:

Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier on windows.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Unspecified errors in the MySQL Server component via unknown vectors related to DDL, Server : Security : Privileges, Server : Security : Encryption, InnoDB : DML.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805171
Version used: `2022-04-14T06:42:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2015-2573`
`cve: CVE-2015-2568`
`cve: CVE-2015-0441`
`cve: CVE-2015-0433`
`url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html`
`url: http://www.securityfocus.com/bid/74078`
`url: http://www.securityfocus.com/bid/74073`
`url: http://www.securityfocus.com/bid/74103`
`url: http://www.securityfocus.com/bid/74089`
`cert-bund: CB-K15/1546`
`cert-bund: CB-K15/1202`
`cert-bund: CB-K15/1193`
`cert-bund: CB-K15/1045`
`cert-bund: CB-K15/1042`
`cert-bund: CB-K15/0964`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0531`
`dfn-cert: DFN-CERT-2015-1623`
`dfn-cert: DFN-CERT-2015-1272`
`dfn-cert: DFN-CERT-2015-1264`
`dfn-cert: DFN-CERT-2015-1105`
`dfn-cert: DFN-CERT-2015-1096`
`dfn-cert: DFN-CERT-2015-1016`
`dfn-cert: DFN-CERT-2015-0758`
`dfn-cert: DFN-CERT-2015-0551`

Medium (CVSS: 4.9)
NVT: Oracle MySQL Security Update (cpujul2018 - 04) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`

... continues on next page ...

... continued from previous page ...

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle MySQL version 5.5.60 and earlier.

Vulnerability Insight
Multiple flaws exist due to an error in the 'Server: Security: Privileges' component of MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Security Update (cpujul2018 - 04) - Windows
OID:1.3.6.1.4.1.25623.1.0.813710
Version used: 2022-08-22T10:11:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2018-3063
url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL
advisory-id: cpujul2018
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K18/0795

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2018-1649
dfn-cert: DFN-CERT-2018-1402

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpujan2021) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.51
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.51, 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.32 and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.145224
Version used: 2021-08-26T13:01:12Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2021-2022
cve: CVE-2021-2060
url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL
advisory-id: cpujan2021
cert-bund: WID-SEC-2023-0067
cert-bund: CB-K21/0062
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0131

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to an unspecified vulnerability.

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

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Replication.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 .
↪..

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.804034
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-5807
url: http://secunia.com/advisories/55327
url: http://www.securityfocus.com/bid/63105
url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
cert-bund: CB-K14/0187
cert-bund: CB-K13/1072
cert-bund: CB-K13/0840
cert-bund: CB-K13/0789
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1846
dfn-cert: DFN-CERT-2013-1795

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.31
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.31, 8.0.18 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server version 5.7.30 and prior and 8.0 through 8.0.17.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145804
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2021-2160`
`url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL`
`advisory-id: cpuapr2021`
`cert-bund: WID-SEC-2023-0065`
`cert-bund: CB-K21/0421`
`dfn-cert: DFN-CERT-2021-0821`

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version: 5.7.34`
`Installation`
`path / port: 3306/tcp`

Solution:
Solution type: VendorFix
Update to version 5.7.34 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server version 5.7.33 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows`
OID:1.3.6.1.4.1.25623.1.0.145802
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2021-2154`
`url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL`
`advisory-id: cpuapr2021`
`cert-bund: WID-SEC-2023-0065`
`cert-bund: CB-K21/0421`
`dfn-cert: DFN-CERT-2022-1241`
`dfn-cert: DFN-CERT-2022-0933`
`dfn-cert: DFN-CERT-2022-0666`
`dfn-cert: DFN-CERT-2021-1660`
`dfn-cert: DFN-CERT-2021-0984`
`dfn-cert: DFN-CERT-2021-0821`

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpujan2021) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version: 5.6.51`
`Installation`
`path / port: 3306/tcp`

Impact

... continues on next page ...

... continued from previous page ...

Successful attacks of this vulnerability can result in the unauthorized ability to cause a hang or frequently repeatedly crash (complete DOS) the MySQL Server.

Solution:
Solution type: VendorFix
Update to version 5.6.51, 5.7.31, 8.0.18 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.30 and 8.0 through 8.0.17.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145222
Version used: `2021-08-26T13:01:12Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2021-2001`
`url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL`
`advisory-id: cpujan2021`
`cert-bund: WID-SEC-2023-0067`
`cert-bund: CB-K21/0062`
`dfn-cert: DFN-CERT-2021-2155`
`dfn-cert: DFN-CERT-2021-0810`
`dfn-cert: DFN-CERT-2021-0131`

Medium (CVSS: 4.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.807924
Version used: 2022-08-31T10:10:28Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-0666
cve: CVE-2016-0647
cve: CVE-2016-0648
cve: CVE-2016-0642
cve: CVE-2016-0643
cve: CVE-2016-2047
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1129
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0791
cert-bund: CB-K16/0750
cert-bund: CB-K16/0646
cert-bund: CB-K16/0597
cert-bund: CB-K16/0493
cert-bund: CB-K16/0133
dfn-cert: DFN-CERT-2016-1204
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0903
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0803
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0143
```

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.40
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.40, 8.0.17 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.16.

Vulnerability Detection Method

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

Details: `Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Wi.
↪..`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.118384
Version used: 2022-10-24T10:14:58Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-21589
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.37
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118382

... continues on next page ...

... continued from previous page ...

Version used: 2022-10-24T10:14:58Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-21595
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2023-0504
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.5.30, 5.6.11 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.29 and 5.6 through 5.6.10.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) .
↪..

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.117213
Version used: 2021-02-12T11:09:59Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-1523
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.40, 8.0.30 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.29.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118386

... continues on next page ...

... continued from previous page ...

Version used: 2022-10-24T10:14:58Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2022-21592
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.4)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.53 and earlier on Windows

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw exists due to an unspecified error in sub component 'Server: Charsets'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.809869
Version used: 2022-10-31T10:12:00Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2017-3243
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95538
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0090

Medium (CVSS: 4.3)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality via unknown vectors.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier on Windows

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server : Pluggable Auth and Server : Security : Privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15`
OID:1.3.6.1.4.1.25623.1.0.805930
Version used: `2022-04-14T06:42:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2015-4737`
`cve: CVE-2015-2620`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html`
`url: http://www.securityfocus.com/bid/75802`
`url: http://www.securityfocus.com/bid/75837`
`cert-bund: CB-K15/1518`
`cert-bund: CB-K15/1202`
`cert-bund: CB-K15/1193`
`cert-bund: CB-K15/1045`
`cert-bund: CB-K15/1020`
`dfn-cert: DFN-CERT-2015-1604`
`dfn-cert: DFN-CERT-2015-1272`
`dfn-cert: DFN-CERT-2015-1264`
`dfn-cert: DFN-CERT-2015-1096`
`dfn-cert: DFN-CERT-2015-1071`

Medium (CVSS: 4.2)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`

... continues on next page ...

... continued from previous page ...

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, 5.7.18 and earlier, on Windows

Vulnerability Insight
Multiple flaws exist due to
- A flaw in the Client mysqldump component.
- A flaw in the Server: DDL component.
- A flaw in the C API component.
- A flaw in the Connector/C component.
- A flaw in the Server: Charsets component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows
OID:1.3.6.1.4.1.25623.1.0.811432
Version used: 2023-03-24T10:19:42Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2017-3651
cve: CVE-2017-3653
cve: CVE-2017-3652

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-3635
cve: CVE-2017-3648
cve: CVE-2017-3641
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
↪#AppendixMSQL
url: http://www.securityfocus.com/bid/99802
url: http://www.securityfocus.com/bid/99810
url: http://www.securityfocus.com/bid/99805
url: http://www.securityfocus.com/bid/99730
url: http://www.securityfocus.com/bid/99789
url: http://www.securityfocus.com/bid/99767
cert-bund: CB-K18/0224
cert-bund: CB-K17/1870
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1453
cert-bund: CB-K17/1401
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior and 5.6 through 5.6.27.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.806877
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-0596
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81176
url: http://www.securityfocus.com/bid/81198
url: http://www.securityfocus.com/bid/81130
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-1192

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0143
dfn-cert: DFN-CERT-2016-0104

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.39
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Update to version 5.5.39 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5.38 and prior.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to SERVER:DDL.

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

... continues on next page ...

... continued from previous page ...

Details: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows
OID:1.3.6.1.4.1.25623.1.0.804783
Version used: 2022-04-14T11:24:11Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2014-6520
url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL
url: http://www.securityfocus.com/bid/70510
advisory-id: cpuoct2014
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1412
cert-bund: CB-K14/1299
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2014-1567
dfn-cert: DFN-CERT-2014-1500
dfn-cert: DFN-CERT-2014-1489
dfn-cert: DFN-CERT-2014-1357

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior.

Vulnerability Insight
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117190
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2016-0616`
`url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL`
`advisory-id: cpujan2016`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0493`
`cert-bund: CB-K16/0246`
`cert-bund: CB-K16/0245`
`cert-bund: CB-K16/0133`
`cert-bund: CB-K16/0094`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0532`
`dfn-cert: DFN-CERT-2016-0266`
`dfn-cert: DFN-CERT-2016-0265`
`dfn-cert: DFN-CERT-2016-0143`
`dfn-cert: DFN-CERT-2016-0104`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.24
Installation
path / port: 3306/tcp

Impact
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'GIS Extension' package / privilege.

Solution:
Solution type: VendorFix
Update to version 5.1.63, 5.5.24 or later.

Affected Software/OS
Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - .
↪..
OID:1.3.6.1.4.1.25623.1.0.117265
Version used: 2021-03-18T11:53:07Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-0540
cve: CVE-2012-1734
cve: CVE-2012-2749

... continues on next page ...

... continued from previous page ...

```
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.23
Installation
path / port:       3306/tcp
```

Impact

The flaw allows remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' package / privilege.

Solution:

Solution type: VendorFix

Update to version 5.1.63, 5.5.23 or later.

Affected Software/OS

Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.

Vulnerability Detection Method

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

Details: `Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - .
↪..`

OID:1.3.6.1.4.1.25623.1.0.117263

Version used: `2021-03-18T11:53:07Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.5.20-log`

... continues on next page ...

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-1689
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.5.31, 5.6.11 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.10.

Vulnerability Insight
Unspecified error in some unknown vectors related to Stored Procedure.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) .
↪..
OID:1.3.6.1.4.1.25623.1.0.809815
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-2376
cve: CVE-2013-1511
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59227
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.5.30 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.29.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117215
Version used: `2021-02-12T11:09:59Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-1512`
`cve: CVE-2013-1526`
`url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL`
`advisory-id: cpuapr2013`
`dfn-cert: DFN-CERT-2013-0798`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20`

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to DLL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805135
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-0391
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72205
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/1193
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 July14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20-log
Vulnerable range: 5.5 - 5.5.37

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.37 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to ENARC and SROPTZR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 July14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804723
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-2494`
`cve: CVE-2014-4207`
`url: http://secunia.com/advisories/59521`
`url: http://www.securityfocus.com/bid/68579`
`url: http://www.securityfocus.com/bid/68593`
`url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi`
`↪ty_patches`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A`
`↪ppendixMSQL`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/0891`
`cert-bund: CB-K14/0868`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-0930`
`dfn-cert: DFN-CERT-2014-0911`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server version 5.5.40 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Server:InnoDB:DDL:Foreign Key

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805133
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-0432
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72217
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html

. . . continues on next page . . .

... continued from previous page ...

cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Optimizer, InnoDB, and Locking.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804076

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-14T11:24:11Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2014-0386
cve: CVE-2014-0393
cve: CVE-2014-0402
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64877
url: http://www.securityfocus.com/bid/64904
url: http://www.securityfocus.com/bid/64908
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0177
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0180
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 04 Jan14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to InnoDB, Optimizer, Error Handling, and some unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 04 Jan14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804075
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-0401`
`cve: CVE-2014-0412`
`cve: CVE-2014-0437`
`cve: CVE-2013-5908`
`url: http://secunia.com/advisories/56491`
`url: http://www.securityfocus.com/bid/64849`
`url: http://www.securityfocus.com/bid/64880`
`url: http://www.securityfocus.com/bid/64896`
`url: http://www.securityfocus.com/bid/64898`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html`
`cert-bund: CB-K15/1518`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K14/0177`
`cert-bund: CB-K14/0082`
`cert-bund: CB-K14/0074`
`cert-bund: CB-K14/0055`
`dfn-cert: DFN-CERT-2015-1604`
`dfn-cert: DFN-CERT-2014-0742`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0180
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.33 and earlier on Windows, Oracle MySQL version 5.6.13 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804074
Version used: 2022-04-14T11:24:11Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2013-5891
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64891
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.35 and earlier and 5.6.15 and earlier on Windows.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Unspecified errors in the MySQL Server component via unknown vectors related to Partition, Replication and XML subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804574
Version used: `2022-04-14T11:24:11Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2014-0384`
`cve: CVE-2014-2419`
`cve: CVE-2014-2438`
`url: http://secunia.com/advisories/57940`
`url: http://www.securityfocus.com/bid/66835`
`url: http://www.securityfocus.com/bid/66846`
`url: http://www.securityfocus.com/bid/66880`
`url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638`
`url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0464`
`cert-bund: CB-K14/0452`
`dfn-cert: DFN-CERT-2014-0742`
`dfn-cert: DFN-CERT-2014-0477`
`dfn-cert: DFN-CERT-2014-0459`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version:  Apply the patch`

... continues on next page ...

... continued from previous page ...

Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.44 and earlier on windows

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805771
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-4816
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77134
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1638

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier on windows

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805764
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2015-4913
cve: CVE-2015-4830
cve: CVE-2015-4826
cve: CVE-2015-4815
cve: CVE-2015-4807
cve: CVE-2015-4802
cve: CVE-2015-4792
cve: CVE-2015-4870
cve: CVE-2015-4861
cve: CVE-2015-4858
cve: CVE-2015-4836
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77153
url: http://www.securityfocus.com/bid/77228
url: http://www.securityfocus.com/bid/77237
url: http://www.securityfocus.com/bid/77222
url: http://www.securityfocus.com/bid/77205
url: http://www.securityfocus.com/bid/77165
url: http://www.securityfocus.com/bid/77171
url: http://www.securityfocus.com/bid/77208
url: http://www.securityfocus.com/bid/77137
url: http://www.securityfocus.com/bid/77145
url: http://www.securityfocus.com/bid/77190
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 Jul15

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow an authenticated remote attacker to cause denial-of-service attack.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on Windows.

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to DML, Server : I_S, Server : Optimizer, and GIS.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-02 Jul15
OID:1.3.6.1.4.1.25623.1.0.805929
Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2015-2648

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2015-4752
cve: CVE-2015-2643
cve: CVE-2015-2582
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75822
url: http://www.securityfocus.com/bid/75849
url: http://www.securityfocus.com/bid/75830
url: http://www.securityfocus.com/bid/75751
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-04 July-2013 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
MySQL is prone to an unspecified vulnerability.

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier and 5.6.10 on Windows.

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Server Options.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerability-04 July-2013 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803726
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-3808`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61227`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-06 July-2013 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
MySQL is prone to an unspecified vulnerability.

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL 5.5.31 and earlier on Windows.

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Server Parser.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerability-06 July-2013 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803728
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-3783`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61210`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities-03 Nov12 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version:  Apply the patch`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data.

Solution:
Solution type: VendorFix
Apply the patch from the referenced vendor advisory or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.63 and Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component vectors related to InnoDB plugin, server full text search and InnoDB.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities-03 Nov12 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803113
Version used: `2022-04-27T12:01:52Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2012-3173`
`cve: CVE-2012-3167`
`cve: CVE-2012-3166`
`url: http://secunia.com/advisories/51008/`
`url: http://www.securityfocus.com/bid/56018`
`url: http://www.securityfocus.com/bid/56028`
`url: http://www.securityfocus.com/bid/56041`
`url: http://www.securelist.com/en/advisories/51008`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html`
`url: https://support.oracle.com/rs?type=doc&id=1475188.1`
`dfn-cert: DFN-CERT-2012-2200`
`dfn-cert: DFN-CERT-2012-2118`

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-02 July-2013 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

Summary
MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow remote authenticated users to affect integrity and availability via unknown vectors and cause denial of service.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.5.31 and earlier, 5.6.11 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Server Replication, Audit Log and Data Manipulation Language.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerabilities-02 July-2013 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803724
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-3812`
`cve: CVE-2013-3809`
`cve: CVE-2013-3793`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61249`
`url: http://www.securityfocus.com/bid/61264`
`url: http://www.securityfocus.com/bid/61272`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-01 July-2013 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, 5.6.11 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Full Text Search and Server Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-01 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803723
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2013-3804
cve: CVE-2013-3802
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61244
url: http://www.securityfocus.com/bid/61260
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: MySQL Server Component Partition Unspecified Vulnerability

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
MySQL is prone to an unspecified vulnerability.

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

Impact
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL version 5.5.x before 5.5.22

Vulnerability Insight
Unspecified error in MySQL Server component related to Partition.

Vulnerability Detection Method
Details: MySQL Server Component Partition Unspecified Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.803801
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2012-1697
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53064
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability Oct-2013 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to an unspecified vulnerability.

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

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL versions 5.1.51 through 5.1.70, 5.5.10 through 5.5.32, and 5.6.x through 5.6.12 on Windows.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability Oct-2013 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804033
Version used: `2022-04-25T14:50:49Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2013-3839`
`url: http://secunia.com/advisories/55327`
`url: http://www.securityfocus.com/bid/63109`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0840`
`cert-bund: CB-K13/0806`
`cert-bund: CB-K13/0789`
`dfn-cert: DFN-CERT-2014-0190`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1846`
`dfn-cert: DFN-CERT-2013-1815`
`dfn-cert: DFN-CERT-2013-1795`

[return to 10.0.0.21]

2.1.26 Medium 49234/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result
`The remote SSH server supports the following weak KEX algorithm(s):`
`KEX algorithm | Reason`

... continues on next page ...

... continued from previous page ...

```
--------------------------------------------------------------------------------
↪---
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SH
↪A-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2022-12-08T10:12:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple`
`↪m`
`url: https://datatracker.ietf.org/doc/html/rfc6194`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
blowfish-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
blowfish-cbc
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

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
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- none algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2022-12-09T10:11:04Z`

References
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`
`url: https://www.kb.cert.org/vuls/id/958563`

[return to 10.0.0.21]

2.1.27 Medium 4848/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)              | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)            | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                        | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 04A9972F
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)  | None
valid from                       | 2013-05-15 05:33:38 UTC
valid until                      | 2023-05-13 05:33:38 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

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

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

. . . continues on next page . . .

... continued from previous page ...

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2021-11-15T10:28:20Z`

References
```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://orchilles.com/ssl-renegotiation-dos/
```

... continues on next page ...

... continued from previous page ...

```
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

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 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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: `2021-11-22T15:32:39Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

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.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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 the references).
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.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

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: 2021-02-12T06:42:15Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 10.0.0.21]

2.1.28 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

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/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 9740980
Packet 2: 9741088

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 implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

... continues on next page ...

... continued from previous page ...

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-05-11T09:09:33Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[return to 10.0.0.21]

2.1.29 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.0.21]

2.1.30 Low 8585/tcp

Low (CVSS: 3.6)
NVT: PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function.

Vulnerability Detection Result
```
Installed version: 5.3.10
Fixed version:     7.2.33
Installation
path / port:       8585/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Affected Software/OS
PHP versions prior 7.2.33, 7.3 prior 7.3.21 and 7.4 prior to 7.4.9.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The phar_parse_zipfile function had use-after-free vulnerability because of mishandling of the actual_alias variable.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.144366
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.3.10`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2020-7068`
`url: https://www.php.net/ChangeLog-7.php#7.2.33`
`url: https://www.php.net/ChangeLog-7.php#7.3.21`
`url: https://www.php.net/ChangeLog-7.php#7.4.9`
`cert-bund: WID-SEC-2022-2116`
`cert-bund: CB-K20/0788`
`dfn-cert: DFN-CERT-2022-2639`
`dfn-cert: DFN-CERT-2022-2638`
`dfn-cert: DFN-CERT-2021-2373`
`dfn-cert: DFN-CERT-2021-1645`
`dfn-cert: DFN-CERT-2021-1453`
`dfn-cert: DFN-CERT-2021-0380`
`dfn-cert: DFN-CERT-2020-1910`
`dfn-cert: DFN-CERT-2020-1732`

Low (CVSS: 3.3)
NVT: WordPress Ninja Forms Contact Form Plugin < 3.6.22 XSS Vulnerability

Summary
The WordPress plugin 'Ninja Forms Contact Form' is prone to a cross-site scripting (XSS) vulnerability

Vulnerability Detection Result
```
Installed version: 2.9.42
Fixed version:     3.6.22
Installation
path / port:       /wordpress/wp-content/plugins/ninja-forms
```

Solution:
Solution type: VendorFix
Update to version 3.6.22 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress Ninja Forms Contact Form plugin prior to version 3.6.22.

Vulnerability Insight
The plugin does not properly escape user input before outputting it back in an admin page, leading to a reflected cross-site scripting (XSS) which could be used against high privilege users such as admin.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Ninja Forms Contact Form Plugin < 3.6.22 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.127430
Version used: `2023-05-17T09:09:49Z`

References
`cve: CVE-2023-1835`
`url: https://wpscan.com/vulnerability/b5fc223c-5ec0-44b2-b2f6-b35f9942d341`

Low (CVSS: 3.1)
NVT: WordPress Multiple Vulnerabilities - June20 (Windows)

Summary
WordPress is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.6.1
Fixed version:     4.6.19
Installation
path / port:       /wordpress
```

Solution:
Solution type: VendorFix
Update to version 3.7.34, 3.8.34, 3.9.32, 4.0.31, 4.1.31, 4.2.28, 4.3.24, 4.4.23, 4.5.22, 4.6.19, 4.7.18, 4.8.14, 4.9.15, 5.0.10, 5.1.6, 5.2.7, 5.3.4, 5.4.2 or later.

Affected Software/OS
WordPress versions 3.7 - 5.4.1.

Vulnerability Insight
WordPress is prone to multiple vulnerabilities:
- Authenticated users with upload permissions (like authors) are able to inject JavaScript into some media file attachment pages in a certain way. This can lead to script execution in the context of a higher privileged user when the file is viewed by them. (CVE-2020-4047)

... continues on next page ...

... continued from previous page ...

- Due to an issue in wp_validate_redirect() and URL sanitization, an arbitrary external link can be crafted leading to unintended/open redirect when clicked. (CVE-2020-4048)
- When uploading themes, the name of the theme folder can be crafted in a way that could lead to JavaScript execution in /wp-admin on the themes page. This does require an admin to upload the theme, and is low severity self-XSS. (CVE-2020-4049)
- Misuse of the 'set-screen-option' filter's return value allows arbitrary user meta fields to be saved. It does require an admin to install a plugin that would misuse the filter. Once installed, it can be leveraged by low privileged users. (CVE-2020-4050)
- Comments from a post or page can sometimes be seen in the latest comments even if the post or page is not public. (CVE-2020-25286)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Multiple Vulnerabilities - June20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.144103
Version used: `2023-03-01T10:20:05Z`

References
`cve: CVE-2020-4047`
`cve: CVE-2020-4048`
`cve: CVE-2020-4049`
`cve: CVE-2020-4050`
`cve: CVE-2020-25286`
`url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2`
`↪w-5m27-wm27`
`url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6p`
`↪w-gvf4-5fj5`
`url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h`
`↪4-phjv-rm6p`
`url: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vp`
`↪v-fgg2-gcqc`
`cert-bund: CB-K20/0583`
`dfn-cert: DFN-CERT-2020-1991`
`dfn-cert: DFN-CERT-2020-1263`

Low (CVSS: 2.6)
NVT: PHP pdo_sql_parser.re 'PDO' extension DoS vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.3.10`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial of service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.3.10
Fixed version: 5.3.14/5.4.4

Impact
Successful exploitation could allow remote attackers to cause a denial of service condition.

Solution:
Solution type: VendorFix
Update to PHP Version 5.3.14 or 5.4.4 or later.

Affected Software/OS
PHP version before 5.3.14 and 5.4.x before 5.4.4 on Windows

Vulnerability Insight
The flaw is due to an error in the PDO extension in pdo_sql_parser.re file, which fails to determine the end of the query string during parsing of prepared statements.

Vulnerability Detection Method
Details: PHP pdo_sql_parser.re 'PDO' extension DoS vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.802670
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:php:php:5.3.10
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2012-3450
url: http://seclists.org/bugtraq/2012/Jun/60
url: http://www.securityfocus.com/bid/54777
url: http://www.php.net/ChangeLog-5.php
url: https://bugs.php.net/bug.php?id=61755
url: https://bugzilla.novell.com/show_bug.cgi?id=769785
dfn-cert: DFN-CERT-2012-1654
dfn-cert: DFN-CERT-2012-1560

[return to 10.0.0.21]

2.1.31 Low 9200/tcp

Low (CVSS: 3.1)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.13
Installation
path / port:       /
```

Impact
This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.13, 7.9.2 or later.

Affected Software/OS
Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.

Vulnerability Insight
A document disclosure flaw was found in Elasticsearch when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)`
OID:1.3.6.1.4.1.25623.1.0.117181
Version used: `2021-08-17T12:00:57Z`

References
```
cve: CVE-2020-7020
url: https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update
↪/253033
url: https://www.elastic.co/community/security
cert-bund: WID-SEC-2022-0607
dfn-cert: DFN-CERT-2022-1530
```

[return to 10.0.0.21]

2.1.32 Low 3306/tcp

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpujul2016) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

Vulnerability Insight
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Connection' sub-component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.808593
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2016-5444
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91987
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169
```

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (cpujul2016) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.10.

Vulnerability Insight

An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Security Encryption' sub-component.

Vulnerability Detection Method

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

Details: `Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (.`

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.808594
Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2016-3452
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91999
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169

Low (CVSS: 3.5)
NVT: Oracle MySQL Server Multiple Vulnerabilities-05 Nov12 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information and manipulate certain data.

Solution:
Solution type: VendorFix
Apply the patch from the linked references or upgrade to latest version.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
The flaw is due to unspecified error in MySQL server component vectors server.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities-05 Nov12 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803115
Version used: `2022-04-27T12:01:52Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2012-3156`
`url: http://secunia.com/advisories/51008/`
`url: http://www.securityfocus.com/bid/56013`
`url: http://www.securelist.com/en/advisories/51008`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html`
`url: https://support.oracle.com/rs?type=doc&id=1475188.1`

Low (CVSS: 3.5)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to affect integrity via unknown vectors.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on windows

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805770
Version used: `2022-04-14T06:42:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2015-4864`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html`
`url: http://www.securityfocus.com/bid/77187`
`cert-bund: CB-K16/0245`
`cert-bund: CB-K15/1844`
`cert-bund: CB-K15/1554`
`dfn-cert: DFN-CERT-2016-0265`
`dfn-cert: DFN-CERT-2015-1946`
`dfn-cert: DFN-CERT-2015-1638`

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-04 Jul15

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation will allow an authenticated remote attacker to cause denial of service attack.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on Windows.

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server : Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Unspecified Vulnerability-04 Jul15`
OID:1.3.6.1.4.1.25623.1.0.805931
Version used: `2022-04-14T06:42:08Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
cve: CVE-2015-4757
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75759
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
```

Low (CVSS: 3.3)
NVT: Oracle MySQL Security Update (cpujul2018 - 02) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Oracle MySQL version 5.5.60 and earlier, 5.6.40 and earlier, 5.7.22 and earlier.

Vulnerability Insight
Multiple flaws exist due to errors in 'Server: Security: Encryption', 'Server: Options', 'MyISAM', 'Client mysqldump' components of application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Security Update (cpujul2018 - 02) - Windows
OID:1.3.6.1.4.1.25623.1.0.813706
Version used: 2022-08-31T10:10:28Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2018-2767

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2018-3066
cve: CVE-2018-3058
cve: CVE-2018-3070
url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL
advisory-id: cpujul2018
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K18/0795
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-1649
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0913
```

Low (CVSS: 3.3)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

Product detection result

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

Summary

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.41
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.40 and prior and 8.x through 8.0.31.

Vulnerability Detection Method

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

Details: `Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.`

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.149532
Version used: 2023-04-19T10:19:33Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2023-21963
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-1033
dfn-cert: DFN-CERT-2023-0885

Low (CVSS: 2.8)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle MySQL version 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Replication.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804077
Version used: 2022-04-14T11:24:11Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2014-0420
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64888
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Windows

Product detection result
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.45
Installation
path / port: 3306/tcp

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 5.6.45, 5.7.19 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.44 and prior and 5.7 through 5.7.18.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.142643
Version used: `2021-09-07T14:01:38Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2019-2730`
`url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL`
`advisory-id: cpujul2019`
`cert-bund: CB-K19/0620`
`dfn-cert: DFN-CERT-2019-2169`
`dfn-cert: DFN-CERT-2019-1453`

Low (CVSS: 1.5)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) - Windows

Product detection result
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version:     5.5.31`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Impact
Successful exploitation will allow local users to affect availability.

Solution:
Solution type: VendorFix
Update to version 5.5.31, 5.6.10 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.9.

Vulnerability Insight
An unspecified error exists in the MySQL Server component via unknown vectors related to Server Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) -.
↪..
OID:1.3.6.1.4.1.25623.1.0.809813
Version used: 2022-04-25T14:50:49Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
cve: CVE-2013-1502
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59239
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798

[return to 10.0.0.21]

2.1.33 Low 49234/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

... continues on next page ...

... continued from previous page ...

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- none algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2021-09-20T11:05:40Z`

[return to 10.0.0.21]