

Scan Report

February 10, 2026

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 “Scan-Windows-Server”. The scan started at Tue Feb 10 20:20:48 2026 UTC and ended at Tue Feb 10 22:11:45 2026 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	2
2	Results per Host	2
2.1	192.168.1.207	2
2.1.1	Critical 8009/tcp	3
2.1.2	Critical 8282/tcp	6
2.1.3	Critical 3306/tcp	13
2.1.4	Critical 9200/tcp	29
2.1.5	Critical 22/tcp	30
2.1.6	Critical general/tcp	32
2.1.7	High 8383/tcp	33
2.1.8	High 8282/tcp	37
2.1.9	High 445/tcp	63
2.1.10	High 4848/tcp	64
2.1.11	High 3306/tcp	68
2.1.12	High 9200/tcp	115
2.1.13	High 22/tcp	116
2.1.14	High 8181/tcp	120
2.1.15	Medium 8383/tcp	124
2.1.16	Medium 3389/tcp	133
2.1.17	Medium 8282/tcp	141
2.1.18	Medium 8022/tcp	156

2.1.19	Medium 4848/tcp	157
2.1.20	Medium 3306/tcp	166
2.1.21	Medium 135/tcp	289
2.1.22	Medium 9200/tcp	292
2.1.23	Medium 22/tcp	297
2.1.24	Medium 8181/tcp	302
2.1.25	Medium 8443/tcp	311
2.1.26	Medium 8020/tcp	318
2.1.27	Low 3306/tcp	319
2.1.28	Low 9200/tcp	330
2.1.29	Low 22/tcp	331
2.1.30	Low general/tcp	332

1 Result Overview

Host	Critical	High	Medium	Low	Log	False P.
192.168.1.207	17	47	134	12	0	0
Total: 1	17	47	134	12	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 included in the report.

Notes are included in 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 210 results selected by the filtering described above. Before filtering there were 375 results.

2 Results per Host

2.1 192.168.1.207

Host scan start Tue Feb 10 20:23:32 2026 UTC

Host scan end Tue Feb 10 22:11:33 2026 UTC

Service (Port)	Threat Level
8009/tcp	Critical
8282/tcp	Critical
3306/tcp	Critical
9200/tcp	Critical
22/tcp	Critical
general/tcp	Critical
8383/tcp	High
8282/tcp	High
445/tcp	High
4848/tcp	High
3306/tcp	High
9200/tcp	High
22/tcp	High
8181/tcp	High
8383/tcp	Medium
3389/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
8282/tcp	Medium
8022/tcp	Medium
4848/tcp	Medium
3306/tcp	Medium
135/tcp	Medium
9200/tcp	Medium
22/tcp	Medium
8181/tcp	Medium
8443/tcp	Medium
8020/tcp	Medium
3306/tcp	Low
9200/tcp	Low
22/tcp	Low
general/tcp	Low

2.1.1 Critical 8009/tcp

Critical (CVSS: 9.8)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check

Summary

Apache Tomcat is prone to a remote code execution (RCE) vulnerability in the AJP connector dubbed 'Ghostcat'.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.

Result:

```
AB v\x0004 Ã\x0088 \x00020K \x0003Â \x0007 =JSESSIONID=5B1151F1A5364E082161FDCE
↳6BADB49F; Path=/; HttpOnly Â \x0001 \x001Ctext/html; charset=ISO-8859-1 Â \x000
↳3 \x00041262 AB\x0004Ã²\x0003\x0004Ã@<?xml version="1.0" encoding="ISO-8859-1"
↳?>
<!--
```

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

... continues on next page ...

...continued from previous page...

```

See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>
</web-app>
AB \x0002\x0005\x0001AB Ã\x0081\x0004 Ã\x0088 \x00020K \x0005
Accept-Ranges \x0005bytes \x0004ETag \x0016W/"1262-1458358374000" Ã \x0005 \x
↳001DSat, 19 Mar 2016 03:32:54 GMT Ã \x0001 \x000Fapplication/xml Ã \x0003 \x00
↳041262 AB\x0004Ã²\x0003\x0004Ã®<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
    http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>
</web-app>
AB \x0002\x0005\x0001

```

Solution:**Solution type:** VendorFix

...continues on next page...

...continued from previous page ...
<ul style="list-style-type: none"> - Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later - For other products using Tomcat please contact the vendor for more information on fixed versions
<p>Affected Software/OS</p> <p>Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wildfly which are using Tomcat might be affected as well.</p>
<p>Vulnerability Insight</p> <p>Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.</p>
<p>Vulnerability Detection Method</p> <p>Sends a crafted AJP request and checks the response. Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check OID:1.3.6.1.4.1.25623.1.0.143545 Version used: 2025-07-11T05:42:17Z</p>
<p>References</p> <p>cve: CVE-2020-1938 url: https://lists.apache.org/thread/bnys5lvgl875dsslkx2vmwxv833l35x url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.31 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.51 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.100 url: https://web.archive.org/web/20250114042903/https://www.chaitin.cn/en/ghostcat url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487 url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/ url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog cisa: Known Exploited Vulnerability (KEV) catalog cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2023-2480 cert-bund: CB-K20/0711 cert-bund: CB-K20/0705 cert-bund: CB-K20/0693 cert-bund: CB-K20/0555 cert-bund: CB-K20/0543 cert-bund: CB-K20/0154 dfn-cert: DFN-CERT-2021-1736 dfn-cert: DFN-CERT-2020-1508 dfn-cert: DFN-CERT-2020-1413 dfn-cert: DFN-CERT-2020-1276 dfn-cert: DFN-CERT-2020-1134</p>
...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[[return to 192.168.1.207](#)]**2.1.2 Critical 8282/tcp****Critical (CVSS: 10.0)****NVT: Apache Tomcat End of Life (EOL) Detection - Windows****Product detection result**

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)**Summary**

The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

The "Apache Tomcat" version on the remote host has reached the end of life.

CPE: cpe:/a:apache:tomcat:8.0.33

Installed version: 8.0.33

Location/URL: 8282/tcp

EOL version: 8.0

EOL date: 2018-06-30

Impact

An EOL version of Apache Tomcat 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 Tomcat version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.

... continues on next page ...

...continued from previous page ...
Details: Apache Tomcat End of Life (EOL) Detection - Windows OID:1.3.6.1.4.1.25623.1.0.108134 Version used: 2025-04-15T05:54:49Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References url: https://tomcat.apache.org/tomcat-10.0-eol.html url: https://tomcat.apache.org/tomcat-85-eol.html url: https://tomcat.apache.org/tomcat-80-eol.html url: https://tomcat.apache.org/tomcat-70-eol.html url: https://tomcat.apache.org/tomcat-60-eol.html url: https://tomcat.apache.org/tomcat-55-eol.html url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases url: https://tomcat.apache.org/whichversion.html
Critical (CVSS: 9.8) NVT: Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows
Summary Apache Tomcat is prone to a rewrite rule bypass vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.104 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.104, 10.1.40, 11.0.6 or later.
Affected Software/OS Apache Tomcat version 9.0.102 and prior, 10.x through 10.1.39 and 11.0.0-M1 through 11.0.5. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
... continues on next page ...

...continued from previous page ...
Vulnerability Insight For a subset of unlikely rewrite rule configurations, it is possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154400 Version used: 2025-05-06T05:40:10Z
References cve: CVE-2025-31651 url: https://lists.apache.org/thread/cpk1vqwvdrp4k9hmd2l3q33j0gzy4fox cert-bund: WID-SEC-2025-2372 cert-bund: WID-SEC-2025-1850 cert-bund: WID-SEC-2025-1572 cert-bund: WID-SEC-2025-1565 cert-bund: WID-SEC-2025-1563 cert-bund: WID-SEC-2025-1439 cert-bund: WID-SEC-2025-1365 cert-bund: WID-SEC-2025-0895 dfn-cert: DFN-CERT-2026-0451 dfn-cert: DFN-CERT-2025-3462 dfn-cert: DFN-CERT-2025-3454 dfn-cert: DFN-CERT-2025-3431 dfn-cert: DFN-CERT-2025-3113 dfn-cert: DFN-CERT-2025-2285 dfn-cert: DFN-CERT-2025-2098 dfn-cert: DFN-CERT-2025-1991 dfn-cert: DFN-CERT-2025-1905 dfn-cert: DFN-CERT-2025-1898 dfn-cert: DFN-CERT-2025-1557 dfn-cert: DFN-CERT-2025-1081
Critical (CVSS: 9.8) NVT: Apache Tomcat RCE Vulnerability (Mar 2025) - Windows
Summary Apache Tomcat is prone to a remote code execution (RCE) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.99
... continues on next page ...

...continued from previous page ...	
Installation	
path / port:	8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.99, 10.1.35, 11.0.3 or later.	
Affected Software/OS Apache Tomcat version 9.0.98 and prior, 10.x through 10.1.34 and 11.0.0-M1 through 11.0.2. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.	
Vulnerability Insight The original implementation of partial PUT used a temporary file based on the user provided file name and path with the path separator replaced by '.'. If all of the following are true, a malicious user is able to view security sensitive files and/or inject content into those files: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - a target URL for security sensitive uploads that is a sub-directory of a target URL for public uploads - attacker knowledge of the names of security sensitive files being uploaded - the security sensitive files also being uploaded via partial PUT If all of the following are true, a malicious user is able to perform remote code execution: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - application is using Tomcat's file based session persistence with the default storage location - application includes a library that may be leveraged in a deserialization attack	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat RCE Vulnerability (Mar 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154161 Version used: 2025-04-11T15:45:04Z	
References cve: CVE-2025-24813 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.3 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.35 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.99 url: https://github.com/iSee857/CVE-2025-24813-PoC	
... continues on next page ...	

...continued from previous page ...
url: https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is-in-the-wild/
url: https://www.openwall.com/lists/oss-security/2025/03/10/5
url: https://scrapco.de/blog/analysis-of-cve-2025-24813-apache-tomcat-path-equiv-alence-rce.html
url: https://bishopfox.com/blog/tomcat-cve-2025-24813-what-you-need-to-know-blog
cert-bund: WID-SEC-2025-1564
cert-bund: WID-SEC-2025-1439
cert-bund: WID-SEC-2025-0825
cert-bund: WID-SEC-2025-0824
cert-bund: WID-SEC-2025-0823
cert-bund: WID-SEC-2025-0511
dfn-cert: DFN-CERT-2025-2098
dfn-cert: DFN-CERT-2025-0993
dfn-cert: DFN-CERT-2025-0890
dfn-cert: DFN-CERT-2025-0888
dfn-cert: DFN-CERT-2025-0766
dfn-cert: DFN-CERT-2025-0622

Critical (CVSS: 9.1) NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windows
Summary Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.37 Installation path / port: 8282/tcp
Impact Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.0.M10 or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, Apache Tomcat versions 8.5.0 to 8.5.4, Apache Tomcat versions 8.0.0.RC1 to 8.0.36, Apache Tomcat versions 7.0.0 to 7.0.70, and Apache Tomcat versions 6.0.0 to 6.0.45 on Windows.
... continues on next page ...

...continued from previous page ...

Vulnerability Insight

Multiple flaws exist due to:

- An error in the system property replacement feature for configuration files.
- An error in the realm implementations in Apache Tomcat that does not process the supplied password if the supplied user name did not exist.
- An error in the configured SecurityManager via a Tomcat utility method that is accessible to web applications.
- An error in the configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.
- An error in the ResourceLinkFactory implementation in Apache Tomcat that does not limit web application access to global JNDI resources to those resources explicitly linked to the web application.

Vulnerability Detection Method

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

Details: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Wind.

↪..

OID:1.3.6.1.4.1.25623.1.0.811298

Version used: 2024-02-15T05:05:40Z

References

cve: CVE-2016-6794

cve: CVE-2016-0762

cve: CVE-2016-5018

cve: CVE-2016-6796

cve: CVE-2016-6797

url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72url: <http://www.securityfocus.com/bid/93940>url: <http://www.securityfocus.com/bid/93944>url: <http://www.securityfocus.com/bid/93939>url: <http://www.securityfocus.com/bid/93942>url: <http://www.securityfocus.com/bid/93943>url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8.5.6

cert-bund: WID-SEC-2022-1910

cert-bund: CB-K17/1060

cert-bund: CB-K17/1033

cert-bund: CB-K17/1031

cert-bund: CB-K17/0659

cert-bund: CB-K17/0397

cert-bund: CB-K17/0133

cert-bund: CB-K16/1927

cert-bund: CB-K16/1673

cert-bund: CB-K16/1646

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-1064
dfn-cert: DFN-CERT-2017-0673
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2016-2035
dfn-cert: DFN-CERT-2016-1772
dfn-cert: DFN-CERT-2016-1743
```

Critical (CVSS: 9.1)

NVT: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability (Apr 2017) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 8.0.33

Fixed version: 8.0.42

Installation

path / port: 8282/tcp

Impact

Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.

Solution:

Solution type: VendorFix

Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M17,

Apache Tomcat versions 8.5.0 to 8.5.11,

Apache Tomcat versions 8.0.0.RC1 to 8.0.41 and

Apache Tomcat versions 7.0.0 to 7.0.75 on Windows

... continues on next page ...

...continued from previous page ...	
Vulnerability Insight	A some calls to application listeners did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability (Apr 2017). ↪.. OID:1.3.6.1.4.1.25623.1.0.810764 Version used: 2025-12-12T15:41:28Z
Product Detection Result	Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References	cve: CVE-2017-5648 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html url: http://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882b↪f6860397368a52600e%3Cannounce.tomcat.apache.org%3E cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0047 cert-bund: CB-K17/1257 cert-bund: CB-K17/1246 cert-bund: CB-K17/1060 cert-bund: CB-K17/0801 cert-bund: CB-K17/0604 dfn-cert: DFN-CERT-2018-0051 dfn-cert: DFN-CERT-2017-1300 dfn-cert: DFN-CERT-2017-1288 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-0828 dfn-cert: DFN-CERT-2017-0624

[\[return to 192.168.1.207 \]](#)

2.1.3 Critical 3306/tcp

Critical (CVSS: 9.8) 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).	
Quality of Detection (QoD): 80%	
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. ↵.. OID:1.3.6.1.4.1.25623.1.0.149536 Version used: 2025-09-09T05:38:49Z	
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-2022-37434 url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL advisory-id: cpuapr2023 cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1653 cert-bund: WID-SEC-2024-1591	
... continues on next page ...	

...continued from previous page...

cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0122
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1783
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-2024-0998
dfn-cert: DFN-CERT-2024-0790
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-1643
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

<p>Critical (CVSS: 9.8) NVT: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.34, 8.1.0 Security Update (cpuoct2023) - Windows</p>
<p>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)</p>
<p>Summary Oracle MySQL Server is prone to multiple vulnerabilities.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.44 Installation path / port: 3306/tcp</p>
<p>Solution: Solution type: VendorFix Update to version 5.7.44, 8.0.35, 8.1.1 or later.</p>
<p>Affected Software/OS Oracle MySQL Server version 5.7.43 and prior, 8.x through 8.0.34 and 8.1.0.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.34, 8.1.0 Security Update (cpuoct2023.↵.. OID:1.3.6.1.4.1.25623.1.0.151218 Version used: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>References cve: CVE-2023-38545 cve: CVE-2023-22084 cve: CVE-2023-38546 url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL advisory-id: cpuoct2023</p>
<p>... continues on next page ...</p>

...continued from previous page...

cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2024-3377
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0893
cert-bund: WID-SEC-2024-0290
cert-bund: WID-SEC-2024-0178
cert-bund: WID-SEC-2024-0175
cert-bund: WID-SEC-2024-0123
cert-bund: WID-SEC-2024-0119
cert-bund: WID-SEC-2024-0110
cert-bund: WID-SEC-2023-2788
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2570
dfn-cert: DFN-CERT-2024-2795
dfn-cert: DFN-CERT-2024-2543
dfn-cert: DFN-CERT-2024-1601
dfn-cert: DFN-CERT-2024-1517
dfn-cert: DFN-CERT-2024-1188
dfn-cert: DFN-CERT-2024-1090
dfn-cert: DFN-CERT-2024-1025
dfn-cert: DFN-CERT-2024-0963
dfn-cert: DFN-CERT-2024-0869
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2024-0376
dfn-cert: DFN-CERT-2024-0220
dfn-cert: DFN-CERT-2024-0185
dfn-cert: DFN-CERT-2024-0184
dfn-cert: DFN-CERT-2024-0181
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2024-0132
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2024-0108
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3064
dfn-cert: DFN-CERT-2023-2988
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2819
dfn-cert: DFN-CERT-2023-2763
dfn-cert: DFN-CERT-2023-2681
dfn-cert: DFN-CERT-2023-2680
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2475
dfn-cert: DFN-CERT-2023-2458

Critical (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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.36 Installation path / port: 3306/tcp	
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: 2025-09-09T05:38:49Z	
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-2021-3711 cve: CVE-2021-22926 cve: CVE-2021-35604 cve: CVE-2021-35624 cve: CVE-2021-22922 cve: CVE-2021-22923	
... continues on next page ...	

...continued from previous page ...

cve: CVE-2021-22924
cve: CVE-2021-22925
cve: CVE-2021-22945
cve: CVE-2021-22946
cve: CVE-2021-22947
cve: CVE-2021-3712
url: <https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL>
advisory-id: cpuoct2021
cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2025-2366
cert-bund: WID-SEC-2025-1459
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0556
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1821
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
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

... continues on next page ...

...continued from previous page ...

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-2025-3324
 dfn-cert: DFN-CERT-2024-0573
 dfn-cert: DFN-CERT-2024-0147
 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
 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

...continues on next page ...

...continued from previous page ...

```

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
dfn-cert: DFN-CERT-2021-1593
dfn-cert: DFN-CERT-2021-1580
dfn-cert: DFN-CERT-2021-1568

```

Critical (CVSS: 9.8)**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)

Summary

Oracle MySQL Server is prone to a vulnerability in libcurl.

...continues on next page ...

...continued from previous page ...	
Quality of Detection (QoD): 80%	
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: 2025-09-09T05:38:49Z	
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-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-2026-0180 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2229 cert-bund: WID-SEC-2023-2031 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	
... continues on next page ...	

...continued from previous page ...

```

cert-bund: WID-SEC-2023-0296
cert-bund: WID-SEC-2023-0189
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1862
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1636
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

```

Critical (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.

Quality of Detection (QoD): 80%**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 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: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

```
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
```

Critical (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.

Quality of Detection (QoD): 80%

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.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:

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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.
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle Mysql Security Update (cpuoct2018 - 02) - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.814258</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2018-3133</p> <p>cve: CVE-2018-3174</p> <p>cve: CVE-2018-3282</p> <p>cve: CVE-2016-9843</p> <p>cve: CVE-2016-9840</p> <p>cve: CVE-2016-9841</p> <p>cve: CVE-2016-9842</p> <p>url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL</p> <p>advisory-id: cpuoct2018</p> <p>cert-bund: WID-SEC-2026-0180</p> <p>cert-bund: WID-SEC-2025-1365</p> <p>cert-bund: WID-SEC-2025-0370</p> <p>cert-bund: WID-SEC-2024-1232</p> <p>cert-bund: WID-SEC-2023-1594</p> <p>cert-bund: WID-SEC-2022-0673</p> <p>cert-bund: CB-K22/0045</p> <p>cert-bund: CB-K20/0714</p> <p>cert-bund: CB-K18/1005</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K18/0030</p> <p>cert-bund: CB-K17/2199</p> <p>cert-bund: CB-K17/2168</p> <p>cert-bund: CB-K17/1745</p> <p>cert-bund: CB-K17/1709</p> <p>cert-bund: CB-K17/1622</p> <p>cert-bund: CB-K17/1585</p> <p>cert-bund: CB-K17/1062</p> <p>cert-bund: CB-K17/0877</p> <p>cert-bund: CB-K17/0784</p>
...continues on next page ...

...continued from previous page ...

```

cert-bund: CB-K16/1996
dfn-cert: DFN-CERT-2026-0129
dfn-cert: DFN-CERT-2025-1437
dfn-cert: DFN-CERT-2025-1423
dfn-cert: DFN-CERT-2024-0998
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

```

Critical (CVSS: 9.0)**NVT: Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - 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.

Quality of Detection (QoD): 80%

... continues on next page ...

...continued from previous page ...
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 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803111 Version used: 2025-09-09T05:38:49Z
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-2012-3197 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
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2012-2118

[\[return to 192.168.1.207 \]](#)**2.1.4 Critical 9200/tcp****Critical (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.

Quality of Detection (QoD): 80%**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: 2025-09-03T08:26:15Z

References

url: <https://www.elastic.co/support/eol>

Critical (CVSS: 9.8)**NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows****Summary**

... continues on next page ...

...continued from previous page ...
Elasticsearch is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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.
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: 2025-09-03T08:26:15Z
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: WID-SEC-2025-2234 cert-bund: CB-K15/1118 dfn-cert: DFN-CERT-2025-2802 dfn-cert: DFN-CERT-2015-1160

[[return to 192.168.1.207](#)]

2.1.5 Critical 22/tcp

Critical (CVSS: 9.8) NVT: OpenSSH < 7.2 X11 Forwarding 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.
Quality of Detection (QoD): 80%
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 Update to 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 < 7.2 X11 Forwarding Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810768 Version used: 2024-12-13T05:05:32Z
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)
... continues on next page ...

...continued from previous page ...

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
 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

[\[return to 192.168.1.207 \]](#)**2.1.6 Critical general/tcp****Critical (CVSS: 10.0)****NVT: Operating System (OS) End of Life (EOL) Detection****Product detection result**

cpe:/o:microsoft:windows_server_2008:r2:sp1
 Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0↵.105937)

Summary

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

The "Windows Server 2008 / Windows Server 2008 R2" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1

Installed version,

...continues on next page ...

...continued from previous page ...	
build or SP:	r2sp1
EOL date:	2020-01-14
EOL info:	https://learn.microsoft.com/en-us/troubleshoot/windows-server/↔/windows-server-eos-faq/end-of-support-windows-server-2008-2008r2
Impact An EOL version of an OS 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: Mitigation Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor. Note / Important: Please create an override for this result if the target host is a: - Windows system with Extended Security Updates (ESU) - System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar	
Vulnerability Detection Method Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2025-05-21T05:40:19Z	
Product Detection Result Product: cpe:/o:microsoft:windows_server_2008:r2:sp1 Method: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937)	

[\[return to 192.168.1.207 \]](#)

2.1.7 High 8383/tcp

High (CVSS: 7.5) NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↔802067)
Summary ... continues on next page ...

...continued from previous page ...
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.
Quality of Detection (QoD): 98%
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) '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)
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
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 All 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 Checks previous collected cipher suites. Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Version used: 2025-03-27T05:38:50Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.802067)
References cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel↵ines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/↵TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch↵eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes↵tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters↵-report-2014 url: https://sweet32.info cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1277 cert-bund: WID-SEC-2024-0209 cert-bund: WID-SEC-2024-0064 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 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
... continues on next page ...

...continued from previous page ...

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-2025-0041
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
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

...continues on next page ...

...continued from previous page ...	
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

[\[return to 192.168.1.207 \]](#)

2.1.8 High 8282/tcp

High (CVSS: 7.8) NVT: Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows
Summary Apache Tomcat is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33
...continues on next page ...

...continued from previous page ...	
Fixed version:	9.0.106
Installation path / port:	8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.106, 10.1.42, 11.0.8 or later.	
Affected Software/OS Apache Tomcat version 9.0.105 and prior, 10.x through 10.1.41 and 11.0.0-M1 through 11.0.7. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.	
Vulnerability Insight The following flaws exist: - CVE-2025-48976: Denial of service (DoS) in Apache Commons FileUpload - CVE-2025-48988: DoS in multipart upload - CVE-2025-49125: Security constraint bypass for pre/post-resources	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154755 Version used: 2025-06-24T05:41:22Z	
References cve: CVE-2025-48976 cve: CVE-2025-48988 cve: CVE-2025-49125 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.8 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.42 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.106 url: https://lists.apache.org/thread/nzkqsok8t42qofgqfmck536mtzyzyp18 url: https://lists.apache.org/thread/m66cytbfrty9k7dc4cg6t11czhsnbywk url: https://www.openwall.com/lists/oss-security/2025/06/16/1 url: https://www.openwall.com/lists/oss-security/2025/06/16/2 url: https://github.com/Samb102/POC-CVE-2025-48988-CVE-2025-48976 cert-bund: WID-SEC-2026-0177 cert-bund: WID-SEC-2026-0175 cert-bund: WID-SEC-2026-0165 cert-bund: WID-SEC-2026-0163 cert-bund: WID-SEC-2026-0162 cert-bund: WID-SEC-2026-0153 cert-bund: WID-SEC-2025-2853	
...continues on next page ...	

...continued from previous page ...	
cert-bund:	WID-SEC-2025-2768
cert-bund:	WID-SEC-2025-2373
cert-bund:	WID-SEC-2025-2372
cert-bund:	WID-SEC-2025-2371
cert-bund:	WID-SEC-2025-2369
cert-bund:	WID-SEC-2025-2366
cert-bund:	WID-SEC-2025-2362
cert-bund:	WID-SEC-2025-2361
cert-bund:	WID-SEC-2025-2360
cert-bund:	WID-SEC-2025-2359
cert-bund:	WID-SEC-2025-2357
cert-bund:	WID-SEC-2025-2356
cert-bund:	WID-SEC-2025-2355
cert-bund:	WID-SEC-2025-2353
cert-bund:	WID-SEC-2025-2351
cert-bund:	WID-SEC-2025-1562
cert-bund:	WID-SEC-2025-1560
cert-bund:	WID-SEC-2025-1559
cert-bund:	WID-SEC-2025-1335
cert-bund:	WID-SEC-2025-1334
dfn-cert:	DFN-CERT-2026-0452
dfn-cert:	DFN-CERT-2026-0451
dfn-cert:	DFN-CERT-2026-0205
dfn-cert:	DFN-CERT-2025-3541
dfn-cert:	DFN-CERT-2025-3168
dfn-cert:	DFN-CERT-2025-2941
dfn-cert:	DFN-CERT-2025-2939
dfn-cert:	DFN-CERT-2025-2390
dfn-cert:	DFN-CERT-2025-2335
dfn-cert:	DFN-CERT-2025-2299
dfn-cert:	DFN-CERT-2025-2291
dfn-cert:	DFN-CERT-2025-2098
dfn-cert:	DFN-CERT-2025-2088
dfn-cert:	DFN-CERT-2025-2056
dfn-cert:	DFN-CERT-2025-1992
dfn-cert:	DFN-CERT-2025-1991
dfn-cert:	DFN-CERT-2025-1780
dfn-cert:	DFN-CERT-2025-1739
dfn-cert:	DFN-CERT-2025-1588

High (CVSS: 7.8) NVT: Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows
Summary Apache Tomcat is prone to a session fixation vulnerability.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.106 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.106, 10.1.42, 11.0.8 or later.
Affected Software/OS Apache Tomcat versions prior to 9.0.106, 10.1.0-M1 through 10.1.41 and 11.0.0-M1 through 11.0.7.
Vulnerability Insight If the rewrite valve was enabled for a web application, an attacker was able to craft a URL that, if a victim clicked on it, would cause the victim's interaction with that resource to occur in the context of the attacker's session.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.127943 Version used: 2025-08-21T05:40:06Z
References cve: CVE-2025-55668 url: https://lists.apache.org/thread/v6bknr96rl711qxkl1c03v0qdvbbqs47 cert-bund: WID-SEC-2025-1905 cert-bund: WID-SEC-2025-1826 dfn-cert: DFN-CERT-2026-0452 dfn-cert: DFN-CERT-2026-0451 dfn-cert: DFN-CERT-2025-1588
High (CVSS: 7.8) NVT: Apache Tomcat DoS Vulnerability (Jul 2025) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
... continues on next page ...

...continued from previous page ...
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.107 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.107 or later.
Affected Software/OS Apache Tomcat version 9.0.106 and prior. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Vulnerability Insight A race condition on connection close could trigger a JVM crash when using the APR/Native connector leading to a DoS. This was particularly noticeable with client initiated closes of HTTP/2 connections.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat DoS Vulnerability (Jul 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154918 Version used: 2025-07-11T15:43:14Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2025-52434 url: https://lists.apache.org/thread/gxgh65004f25y8519coth6w7vchww030 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107 cert-bund: WID-SEC-2026-0177 cert-bund: WID-SEC-2025-1905 cert-bund: WID-SEC-2025-1468 dfn-cert: DFN-CERT-2025-2957
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2025-2390
dfn-cert: DFN-CERT-2025-2299
dfn-cert: DFN-CERT-2025-2056
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1789

High (CVSS: 7.8) NVT: Apache Tomcat DoS Vulnerability (Jul 2024) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.90 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.90, 10.1.25, 11.0.0-M21 or later.
Affected Software/OS Apache Tomcat versions prior to 9.0.90, 10.x through 10.1.24 and 11.0.0-M1 through 11.0.0-M20. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.
Vulnerability Insight When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host.
... continues on next page ...

...continued from previous page ...
Details: Apache Tomcat DoS Vulnerability (Jul 2024) - Windows OID:1.3.6.1.4.1.25623.1.0.152544 Version used: 2024-12-19T05:05:34Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2024-34750 url: https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvp1nl77y8l url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M2 ↪1 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.25 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.90 cert-bund: WID-SEC-2025-0163 cert-bund: WID-SEC-2025-0161 cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0144 cert-bund: WID-SEC-2025-0143 cert-bund: WID-SEC-2024-3197 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1905 cert-bund: WID-SEC-2024-1522 dfn-cert: DFN-CERT-2025-2098 dfn-cert: DFN-CERT-2025-1991 dfn-cert: DFN-CERT-2025-1517 dfn-cert: DFN-CERT-2025-0170 dfn-cert: DFN-CERT-2025-0146 dfn-cert: DFN-CERT-2024-2192 dfn-cert: DFN-CERT-2024-2031 dfn-cert: DFN-CERT-2024-1723

High (CVSS: 7.8) NVT: Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary ... continues on next page ...

...continued from previous page ...
Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.107 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.107, 10.1.43, 11.0.9 or later.
Affected Software/OS Apache Tomcat version 9.0.106 and prior, 10.x through 10.1.42 and 11.0.0-M1 through 11.0.8. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Vulnerability Insight The following flaws exist: - CVE-2025-52520: DoS due to overflow in file upload limit - CVE-2025-53506: DoS via excessive HTTP/2 streams
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154896 Version used: 2025-07-11T15:43:14Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2025-52520 cve: CVE-2025-53506 url: https://lists.apache.org/thread/trqq01bbxw6c92zx69kx2mw2qgmfy0o5 url: https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.43 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.9
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2025-1905
 cert-bund: WID-SEC-2025-1468
 dfn-cert: DFN-CERT-2026-0452
 dfn-cert: DFN-CERT-2026-0451
 dfn-cert: DFN-CERT-2025-2390
 dfn-cert: DFN-CERT-2025-2335
 dfn-cert: DFN-CERT-2025-2299
 dfn-cert: DFN-CERT-2025-2219
 dfn-cert: DFN-CERT-2025-2168
 dfn-cert: DFN-CERT-2025-2088
 dfn-cert: DFN-CERT-2025-2056
 dfn-cert: DFN-CERT-2025-1991
 dfn-cert: DFN-CERT-2025-1789

High (CVSS: 7.8)

NVT: Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)**Summary**

Apache Tomcat is prone to is prone to a denial of service (DoS) vulnerability in the HTTP/2 protocol dubbed 'MadeYouReset'.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 8.0.33

Fixed version: 9.0.108

Installation

path / port: 8282/tcp

Solution:**Solution type:** VendorFix

Update to version 9.0.108, 10.1.44, 11.0.10 or later.

Affected Software/OS

Apache Tomcat version 9.0.107 and prior, 10.x through 10.1.43 and 11.0.0-M1 through 11.0.9.
 Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws.
 If you disagree with this assessment and want to accept the risk please create an override for this result.

... continues on next page ...

...continued from previous page...

Vulnerability Insight

A mismatch caused by client-triggered server-sent stream resets between HTTP/2 specifications and the internal architectures of some HTTP/2 implementations may result in excessive server resource consumption leading to denial-of-service (DoS). By opening streams and then rapidly triggering the server to reset them, using malformed frames or flow control errors, an attacker can exploit incorrect stream accounting. Streams reset by the server are considered closed at the protocol level, even though backend processing continues. This allows a client to cause the server to handle an unbounded number of concurrent streams on a single connection.

Vulnerability Detection Method

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

Details: Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows
OID:1.3.6.1.4.1.25623.1.0.171673

Version used: 2025-08-26T05:39:52Z

Product Detection Result

Product: cpe:/a:apache:tomcat:8.0.33

Method: Apache Tomcat Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2025-8671

cve: CVE-2025-48989

url: <https://lists.apache.org/thread/9ydfg0xr0tchmg1cprhxgwhj0hfwxlyf>

url: <https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0>

url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.108

url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.44

url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.10

url: <https://galbarnahum.com/posts/made-you-reset-intro>

url: <https://deepness-lab.org/publications/madeyoureset/>

url: <https://kb.cert.org/vuls/id/767506>

url: <https://thehackernews.com/2025/08/new-http2-madeyoureset-vulnerability.html>

cert-bund: WID-SEC-2026-0177

cert-bund: WID-SEC-2026-0175

cert-bund: WID-SEC-2026-0173

cert-bund: WID-SEC-2026-0165

cert-bund: WID-SEC-2025-2853

cert-bund: WID-SEC-2025-2373

cert-bund: WID-SEC-2025-2361

cert-bund: WID-SEC-2025-2360

cert-bund: WID-SEC-2025-2357

cert-bund: WID-SEC-2025-2356

cert-bund: WID-SEC-2025-1830

dfn-cert: DFN-CERT-2026-0452

dfn-cert: DFN-CERT-2026-0451

...continues on next page...

...continued from previous page ...

dfn-cert: DFN-CERT-2025-3431
 dfn-cert: DFN-CERT-2025-2957
 dfn-cert: DFN-CERT-2025-2390
 dfn-cert: DFN-CERT-2025-2299
 dfn-cert: DFN-CERT-2025-2224
 dfn-cert: DFN-CERT-2025-2219

High (CVSS: 7.5)

NVT: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)**Summary**

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 8.0.33

Fixed version: 8.5.85

Installation

path / port: 8282/tcp

Solution:**Solution type:** VendorFix

Update to version 8.5.85, 9.0.71, 10.1.5, 11.0.0-M3 or later.

Affected Software/OS

Apache Tomcat versions through 8.5.84, 9.0.0-M1 through 9.0.70, 10.x through 10.1.4 and 11.0.0-M1 only.

Vulnerability Insight

Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

Vulnerability Detection Method

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

Details: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.104551 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2023-24998 url: https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85 url: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrdoy cert-bund: WID-SEC-2025-0810 cert-bund: WID-SEC-2024-1652 cert-bund: WID-SEC-2024-1642 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1622 cert-bund: WID-SEC-2024-1238 cert-bund: WID-SEC-2024-0890 cert-bund: WID-SEC-2024-0888 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0124 cert-bund: WID-SEC-2024-0117 cert-bund: WID-SEC-2024-0054 cert-bund: WID-SEC-2023-2688 cert-bund: WID-SEC-2023-2675 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2309 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1817 cert-bund: WID-SEC-2023-1815 cert-bund: WID-SEC-2023-1813 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1811 cert-bund: WID-SEC-2023-1809 cert-bund: WID-SEC-2023-1808 cert-bund: WID-SEC-2023-1807 cert-bund: WID-SEC-2023-1794 cert-bund: WID-SEC-2023-1792 cert-bund: WID-SEC-2023-1791 cert-bund: WID-SEC-2023-1784
...continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1782
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1142
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1017
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-2025-1992
dfn-cert: DFN-CERT-2024-2151
dfn-cert: DFN-CERT-2024-1865
dfn-cert: DFN-CERT-2024-1006
dfn-cert: DFN-CERT-2024-0059
dfn-cert: DFN-CERT-2024-0048
dfn-cert: DFN-CERT-2023-2778
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2054
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1642
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-2023-0763
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2023-0540
dfn-cert: DFN-CERT-2023-0414

High (CVSS: 7.5)

NVT: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

...continues on next page ...

...continued from previous page ...
Summary Apache Tomcat is prone to a security bypass vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.53 Installation path / port: 8282/tcp
Impact Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52 and 7.0.35 to 7.0.88 on Windows.
Vulnerability Insight The flaw exists due to a missing host name verification when using TLS with the WebSocket client.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.813742 Version used: 2025-09-17T05:39:26Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2018-8034 url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722091057.GA70283@minotaur.apache.org%3E url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53
... continues on next page ...

...continued from previous page ...
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90
cert-bund: WID-SEC-2024-1682
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K19/0907
cert-bund: CB-K19/0616
cert-bund: CB-K19/0320
cert-bund: CB-K18/1005
cert-bund: CB-K18/0809
dfn-cert: DFN-CERT-2019-2418
dfn-cert: DFN-CERT-2019-1627
dfn-cert: DFN-CERT-2019-1237
dfn-cert: DFN-CERT-2019-0951
dfn-cert: DFN-CERT-2019-0451
dfn-cert: DFN-CERT-2019-0147
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1471
dfn-cert: DFN-CERT-2018-1443
dfn-cert: DFN-CERT-2018-1262

High (CVSS: 7.5) NVT: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.36 Installation path / port: 8282/tcp
Impact Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.
Affected Software/OS Apache Tomcat 7.x before 7.0.70, 8.0.0.RC1 before 8.0.36, 8.5.x before 8.5.3, and 9.0.0.M1 before 9.0.0.M7.
Vulnerability Insight The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.808197 Version used: 2022-04-13T13:17:10Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2016-3092 url: http://tomcat.apache.org/security-7.html url: http://www.securityfocus.com/bid/91453 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-9.html cert-bund: WID-SEC-2023-0644 cert-bund: WID-SEC-2022-1537 cert-bund: WID-SEC-2022-1375 cert-bund: CB-K18/0605 cert-bund: CB-K17/1750 cert-bund: CB-K17/1198 cert-bund: CB-K17/1060 cert-bund: CB-K17/0657 cert-bund: CB-K17/0397 cert-bund: CB-K16/1993 cert-bund: CB-K16/1799 cert-bund: CB-K16/1758 cert-bund: CB-K16/1322 cert-bund: CB-K16/1002 cert-bund: CB-K16/0993 dfn-cert: DFN-CERT-2023-0574
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-1905
dfn-cert: DFN-CERT-2016-1823
dfn-cert: DFN-CERT-2016-1407
dfn-cert: DFN-CERT-2016-1068
dfn-cert: DFN-CERT-2016-1059

High (CVSS: 7.5) NVT: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.52 Installation path / port: 8282/tcp
Impact Successful exploitation will allow an attacker to conduct a denial-of-service condition.
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.8 or 8.5.31 or 8.0.52 or 7.0.90 or later. Please see the references for more information.
Affected Software/OS Apache Tomcat 9.0.0.M9 to 9.0.7 Apache Tomcat 8.5.0 to 8.5.30 Apache Tomcat 8.0.0.RC1 to 8.0.51 Apache Tomcat 7.0.28 to 7.0.86 on Windows.
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The flaw exists due to improper handling of overflow in the UTF-8 decoder with supplementary characters.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows OID: 1.3.6.1.4.1.25623.1.0.813724 Version used: 2025-09-17T05:39:26Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2018-1336 url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090435.GA60759%40minotaur.apache.org%3E url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0809 dfn-cert: DFN-CERT-2020-0048 dfn-cert: DFN-CERT-2018-2474 dfn-cert: DFN-CERT-2018-2165 dfn-cert: DFN-CERT-2018-2142 dfn-cert: DFN-CERT-2018-2133 dfn-cert: DFN-CERT-2018-2125 dfn-cert: DFN-CERT-2018-2097 dfn-cert: DFN-CERT-2018-1928 dfn-cert: DFN-CERT-2018-1753 dfn-cert: DFN-CERT-2018-1541 dfn-cert: DFN-CERT-2018-1471 dfn-cert: DFN-CERT-2018-1443 dfn-cert: DFN-CERT-2018-1262
High (CVSS: 7.5) NVT: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Apr 2017) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33
... continues on next page ...

...continued from previous page ...
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.43 Installation path / port: 8282/tcp
Impact Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M18, Apache Tomcat versions 8.5.0 to 8.5.12, Apache Tomcat versions 8.0.0.RC1 to 8.0.42, Apache Tomcat versions 7.0.0 to 7.0.76 and Apache Tomcat versions 6.0.0 to 6.0.52 on Windows.
Vulnerability Insight A bug in the handling of the pipelined requests when send file was used resulted in the pipelined request being lost when send file processing of the previous request completed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Apr 20. ↪.. OID:1.3.6.1.4.1.25623.1.0.810762 Version used: 2025-12-12T15:41:28Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References ... continues on next page ...

...continued from previous page ...
cve: CVE-2017-5647 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html url: http://tomcat.apache.org/security-6.html url: https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0 ↪dee9190ba48171451a0%3Cusers.tomcat.apache.org%3E cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0047 cert-bund: CB-K17/1831 cert-bund: CB-K17/1423 cert-bund: CB-K17/1246 cert-bund: CB-K17/1205 cert-bund: CB-K17/1060 cert-bund: CB-K17/1033 cert-bund: CB-K17/0801 cert-bund: CB-K17/0604 dfn-cert: DFN-CERT-2018-0051 dfn-cert: DFN-CERT-2017-1914 dfn-cert: DFN-CERT-2017-1485 dfn-cert: DFN-CERT-2017-1288 dfn-cert: DFN-CERT-2017-1243 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-1068 dfn-cert: DFN-CERT-2017-0828 dfn-cert: DFN-CERT-2017-0624

High (CVSS: 7.5)

NVT: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 8.0.33

Fixed version: 8.0.41

Installation

path / port: 8282/tcp

Impact

Successful exploitation will allow remote attackers to gain access to potentially sensitive information.

Solution:

... continues on next page ...

...continued from previous page ...	
Solution type: VendorFix	Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.
Affected Software/OS	Apache Tomcat versions 9.0.0.M1 to 9.0.0.M13, Apache Tomcat versions 8.5.0 to 8.5.8, Apache Tomcat versions 8.0.0.RC1 to 8.0.39, Apache Tomcat versions 7.0.0 to 7.0.73, and Apache Tomcat versions 6.0.16 to 6.0.48 on Windows.
Vulnerability Insight	The flaw exists due to error handling of the send file code for the NIO HTTP connector in Apache Tomcat resulting in the current Processor object being added to the Processor cache multiple times. This in turn means that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.811296 Version used: 2024-02-15T05:05:40Z
References	cve: CVE-2016-8745 url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60409 url: http://www.securityfocus.com/bid/94828 url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41 url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9 url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50 cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2022-1375 cert-bund: CB-K18/0605 cert-bund: CB-K17/1746 cert-bund: CB-K17/1060 cert-bund: CB-K17/1033 cert-bund: CB-K17/0801 cert-bund: CB-K17/0444 cert-bund: CB-K17/0397 cert-bund: CB-K17/0303 cert-bund: CB-K17/0133 cert-bund: CB-K17/0090 cert-bund: CB-K16/1929 dfn-cert: DFN-CERT-2018-0729 dfn-cert: DFN-CERT-2017-1822 dfn-cert: DFN-CERT-2017-1095
...continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0308
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-2037

High (CVSS: 7.5) NVT: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability (Mar 2017) - Windows
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.39 Installation path / port: 8282/tcp
Impact Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M17, 8.5.11 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M11 to 9.0.0.M15 and Apache Tomcat versions 8.5.0 to 8.5.9 on Windows.
Vulnerability Insight The refactoring to make wider use of ByteBuffer introduced a regression that could cause information to leak between requests on the same connection. When running behind a reverse proxy, this could result in information leakage between users.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability (Mar 2017) - W. ↪.. OID:1.3.6.1.4.1.25623.1.0.810719
... continues on next page ...

...continued from previous page ...
Version used: 2025-12-12T15:41:28Z
References cve: CVE-2016-8747 url: http://svn.apache.org/viewvc?view=revision&revision=1774161 url: http://www.securityfocus.com/bid/96895 url: http://svn.apache.org/viewvc?view=revision&revision=1774166 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.11 url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M17 cert-bund: CB-K17/0426 dfn-cert: DFN-CERT-2017-0433
High (CVSS: 7.5) NVT: Apache Tomcat Security Bypass Vulnerability - Windows
Summary Apache Tomcat is prone to a security bypass vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.44 Installation path / port: 8282/tcp
Impact Successful exploitation will allow an attacker to exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.
Affected Software/OS Apache Tomcat 9.0.0.M1 to 9.0.0.M20, Apache Tomcat 8.5.0 to 8.5.14, Apache Tomcat 8.0.0.RC1 to 8.0.43 and Apache Tomcat 7.0.0 to 7.0.77 on Windows
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. Tomcat's Default Servlet did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.811140 Version used: 2024-02-15T05:05:40Z</p>
<p>References cve: CVE-2017-5664 url: https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b↪8b7896538478d760660%3Cannounce.tomcat.apache.org%3E url: http://www.securityfocus.com/bid/98888 cert-bund: WID-SEC-2025-1212 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0605 cert-bund: CB-K18/0603 cert-bund: CB-K18/0478 cert-bund: CB-K18/0066 cert-bund: CB-K18/0047 cert-bund: CB-K17/2024 cert-bund: CB-K17/2017 cert-bund: CB-K17/1831 cert-bund: CB-K17/1748 cert-bund: CB-K17/1492 cert-bund: CB-K17/1423 cert-bund: CB-K17/1257 cert-bund: CB-K17/1246 cert-bund: CB-K17/0977 dfn-cert: DFN-CERT-2018-1274 dfn-cert: DFN-CERT-2018-0729 dfn-cert: DFN-CERT-2018-0513 dfn-cert: DFN-CERT-2018-0077 dfn-cert: DFN-CERT-2018-0051 dfn-cert: DFN-CERT-2017-2116 dfn-cert: DFN-CERT-2017-2106 dfn-cert: DFN-CERT-2017-1914 dfn-cert: DFN-CERT-2017-1827 dfn-cert: DFN-CERT-2017-1558 dfn-cert: DFN-CERT-2017-1485</p>
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2017-1300 dfn-cert: DFN-CERT-2017-1288 dfn-cert: DFN-CERT-2017-1011
High (CVSS: 7.1) NVT: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Nov 2016) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.39 Installation path / port: 8282/tcp
Impact Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other than their own.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M11, Apache Tomcat versions 8.5.0 to 8.5.6, Apache Tomcat versions 8.0.0.RC1 to 8.0.38, Apache Tomcat versions 7.0.0 to 7.0.72, and Apache Tomcat versions 6.0.0 to 6.0.47 on Windows.
Vulnerability Insight The code that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host.
... continues on next page ...

...continued from previous page ...	
Details: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Nov 2016). ↔..	
OID:1.3.6.1.4.1.25623.1.0.810717	
Version used: 2025-12-12T15:41:28Z	
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
References cve: CVE-2016-6816 url: https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48 url: http://www.securityfocus.com/bid/94461 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13 url: https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat- ↔information-disclosure cert-bund: WID-SEC-2025-0215 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K17/1746 cert-bund: CB-K17/1060 cert-bund: CB-K17/1033 cert-bund: CB-K17/0444 cert-bund: CB-K17/0397 cert-bund: CB-K17/0198 cert-bund: CB-K17/0133 cert-bund: CB-K17/0090 cert-bund: CB-K16/1976 cert-bund: CB-K16/1927 cert-bund: CB-K16/1815 dfn-cert: DFN-CERT-2017-1822 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-1068 dfn-cert: DFN-CERT-2017-0456 dfn-cert: DFN-CERT-2017-0404 dfn-cert: DFN-CERT-2017-0203 dfn-cert: DFN-CERT-2017-0137 dfn-cert: DFN-CERT-2017-0095 dfn-cert: DFN-CERT-2016-2090 dfn-cert: DFN-CERT-2016-2035 dfn-cert: DFN-CERT-2016-1922	

[[return to 192.168.1.207](#)]

2.1.9 High 445/tcp

<p>High (CVSS: 8.8) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)</p>
<p>Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.</p>
<p>Quality of Detection (QoD): 95%</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>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.</p>
<p>Solution: Solution type: VendorFix The vendor has released updates. Please see the references for more information.</p>
<p>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</p>
<p>Vulnerability Insight Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.</p>
<p>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: 2024-07-17T05:05:38Z</p>
<p>References cve: CVE-2017-0143 cve: CVE-2017-0144</p>
<p>... continues on next page ...</p>

...continued from previous page ...

```

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

```

[\[return to 192.168.1.207 \]](#)**2.1.10 High 4848/tcp**

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

Product detection result

```

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

```

Summary

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

Quality of Detection (QoD): 98%

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)
'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)

```

... continues on next page ...

...continued from previous page ...
<p>'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:</p> <p>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</p>
<p>Impact</p> <p>This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS</p> <p>All services accepting vulnerable SSL/TLS cipher suites via HTTPS.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the vulnerable cipher suites:</p> <p>- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).</p>
<p>Vulnerability Detection Method</p> <p>Checks previous collected cipher suites.</p> <p>Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS</p> <p>OID:1.3.6.1.4.1.25623.1.0.108031</p> <p>Version used: 2025-03-27T05:38:50Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:transport_layer_security</p> <p>Method: SSL/TLS: Report Supported Cipher Suites</p> <p>OID: 1.3.6.1.4.1.25623.1.0.802067)</p>
<p>References</p> <p>cve: CVE-2016-2183</p> <p>cve: CVE-2016-6329</p> <p>cve: CVE-2020-12872</p> <p>url: https://ssl-config.mozilla.org</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html</p> <p>url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandards_node.html</p>
... continues on next page ...

...continued from previous page ...

```

↪tstandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
url: https://sweet32.info
cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
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
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

```

... continues on next page ...

...continued from previous page ...

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-2025-0041
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
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

...continues on next page ...

...continued from previous page ...

```

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 192.168.1.207](#)]**2.1.11 High 3306/tcp****High (CVSS: 8.1)****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.

Quality of Detection (QoD): 80%**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: 2025-09-09T05:38:49Z	
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-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-2026-0180	
cert-bund: WID-SEC-2025-2364	
cert-bund: WID-SEC-2025-1905	
cert-bund: WID-SEC-2025-1550	
cert-bund: WID-SEC-2024-2180	
cert-bund: WID-SEC-2024-1591	
cert-bund: WID-SEC-2023-2229	
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-2025-2944	
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-2022-1241
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
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

```

High (CVSS: 8.1)

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.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 5.5.20

Fixed version: 5.7.39

Installation

path / port: 3306/tcp

... continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z	
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-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-2026-0180	
cert-bund: WID-SEC-2024-1186	
cert-bund: WID-SEC-2024-0794	
cert-bund: WID-SEC-2023-2723	
cert-bund: WID-SEC-2023-2229	
cert-bund: WID-SEC-2023-1969	
cert-bund: WID-SEC-2023-1784	
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	
... continues on next page ...	

...continued from previous page...	
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
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-2024-2686
dfn-cert:	DFN-CERT-2024-2451
dfn-cert:	DFN-CERT-2024-0998
dfn-cert:	DFN-CERT-2024-0790
dfn-cert:	DFN-CERT-2024-0147
dfn-cert:	DFN-CERT-2023-3028
dfn-cert:	DFN-CERT-2023-2667
dfn-cert:	DFN-CERT-2023-2600
dfn-cert:	DFN-CERT-2023-2599
dfn-cert:	DFN-CERT-2023-2571
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
...continues on next page...	

...continued from previous page ...
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
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: 8.1)

NVT: Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (cpu-jul2016) - 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.

Quality of Detection (QoD): 80%

... 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 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: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K16/1742
 cert-bund: CB-K16/1448
 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

High (CVSS: 7.7)

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.

Quality of Detection (QoD): 80%**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

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

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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: 2025-09-09T05:38:49Z
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-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
High (CVSS: 7.7) 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)
...continues on next page ...

...continued from previous page ...
Summary Oracle MySQL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-2017-3309 cve: CVE-2017-3308 cve: CVE-2017-3329 cve: CVE-2017-3456
... continues on next page ...

...continued from previous page ...

```

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
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

```

High (CVSS: 7.5)

NVT: Oracle MySQL Denial Of Service Vulnerability (Feb 2017) - 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 a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
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 (Feb 2017) - Windows OID:1.3.6.1.4.1.25623.1.0.810603 Version used: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

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 Multiple Unspecified vulnerabilities-01 (Feb 2015) - 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.

Quality of Detection (QoD): 80%**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, 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.

... 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-01 (Feb 2015) - Windows
OID:1.3.6.1.4.1.25623.1.0.805132

Version used: 2025-09-09T05:38:49Z

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-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

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 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)

... continues on next page ...

...continued from previous page ...	
Summary	Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
Quality of Detection (QoD): 80%	
Vulnerability Detection Result	Installed version: 5.5.20 Fixed version: 5.5.40 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 5.5.40, 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: 2025-09-09T05:38:49Z
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-2014-6507 cve: CVE-2014-6491 cve: CVE-2014-6500 cve: CVE-2014-6469
... continues on next page ...	

...continued from previous page ...

```

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#AppendixMySQL
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
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: 1.3.6.1.4.1.1.25623.1.0.100152)

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection (QoD): 80%**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 5.5.45 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: 2025-09-09T05:38:49Z	
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-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 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: 1.3.6.1.4.1.1.25623.1.0.100152)
Summary Oracle MySQL Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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: WID-SEC-2026-0205 cert-bund: WID-SEC-2024-0794
... continues on next page ...

...continued from previous page ...

```

cert-bund: WID-SEC-2023-3080
cert-bund: CB-K21/1088
cert-bund: CB-K21/0070
cert-bund: CB-K20/1023
cert-bund: CB-K20/1017
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 <= 5.7.33 / 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.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 5.5.20

Fixed version: 5.7.34

Installation

path / port: 3306/tcp

Solution:

... continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z	
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-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	
cert-bund: WID-SEC-2026-0180	
cert-bund: WID-SEC-2025-0227	
cert-bund: WID-SEC-2024-0794	
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	
...continues on next page ...	

...continued from previous page ...	
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-2024-2451
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
dfn-cert:	DFN-CERT-2021-1803
dfn-cert:	DFN-CERT-2021-1740
dfn-cert:	DFN-CERT-2021-1670
dfn-cert:	DFN-CERT-2021-1660
...continues on next page ...	

```
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
```

NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Windows

```
cpe:/a:mysql:mysql:5.5.20-log
```

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

...continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z	
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-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-2026-0180 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-2229 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	
...continues on next page ...	

...continued from previous page ...
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
dfn-cert: DFN-CERT-2021-1931

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 5.5.20

Fixed version: 5.7.38

Installation

path / port: 3306/tcp

... continues on next page ...

...continued from previous page ...	
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	
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: 2025-09-09T05:38:49Z	
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-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-2026-0180	
cert-bund: WID-SEC-2024-2086	
cert-bund: WID-SEC-2024-1591	
cert-bund: WID-SEC-2024-1186	
cert-bund: WID-SEC-2024-0794	
cert-bund: WID-SEC-2023-1969	
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	
...continues on next page ...	

...continued from previous page ...

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
 dfn-cert: DFN-CERT-2025-3324
 dfn-cert: DFN-CERT-2024-0147
 dfn-cert: DFN-CERT-2023-2667
 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

...continues on next page ...

...continued from previous page ...
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: 7.5) 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.
Quality of Detection (QoD): 80%
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, 8.0.31 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: 2025-09-09T05:38:49Z
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-2023-21912 url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMySQL advisory-id: cpuapr2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-2031 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: 7.5) 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.
Quality of Detection (QoD): 80%
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, 8.0.33 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.↵..
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.149538 Version used: 2025-09-09T05:38:49Z
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-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-2025-1365 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-2086 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0114 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2229 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1886 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1793 cert-bund: WID-SEC-2023-1790 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-2025-3324 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1188 dfn-cert: DFN-CERT-2024-0593 dfn-cert: DFN-CERT-2024-0454 dfn-cert: DFN-CERT-2024-0147
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2024-0126
dfn-cert: DFN-CERT-2024-0016
dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1643
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
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 <= 5.7.42, 8.x <= 8.0.33 Security Update (cpuoct2023) - 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.
Quality of Detection (QoD):	80%
Vulnerability Detection Result	Installed version: 5.5.20 Fixed version: 5.7.43 Installation path / port: 3306/tcp
Solution:	Solution type: VendorFix Update to version 5.7.43, 8.0.34 or later.
Affected Software/OS	Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpuoct2023) - Win. ↔... OID:1.3.6.1.4.1.25623.1.0.151214 Version used: 2025-09-09T05:38:49Z
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-2023-2650 cve: CVE-2023-0464 cve: CVE-2023-0465 cve: CVE-2023-0466 cve: CVE-2023-1255 url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL advisory-id: cpuoct2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0120 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2917
... continues on next page ...	

...continued from previous page ...

cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1781
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1323
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-1053
cert-bund: WID-SEC-2023-0782
cert-bund: WID-SEC-2023-0732
dfn-cert: DFN-CERT-2025-3324
dfn-cert: DFN-CERT-2025-2802
dfn-cert: DFN-CERT-2024-1799
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0565
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2749
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1720
dfn-cert: DFN-CERT-2023-1649
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1245
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0960
dfn-cert: DFN-CERT-2023-0929
dfn-cert: DFN-CERT-2023-0904
dfn-cert: DFN-CERT-2023-0782
dfn-cert: DFN-CERT-2023-0700
dfn-cert: DFN-CERT-2023-0645

High (CVSS: 7.5) NVT: Oracle MySQL Server <= 8.0.39, 8.1 <= 8.4.2, 9.0 <= 9.0.1 Security Update (cpuoct2024) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.40 Installation path / port: 3306/tcp
Solution: Solution type: VendorFix Update to version 8.0.40, 8.4.3, 9.0.2 or later.
Affected Software/OS Oracle MySQL Server version 8.0.39 and prior, 8.1 through 8.4.2 and 9.0 through 9.0.1.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.39, 8.1 <= 8.4.2, 9.0 <= 9.0.1 Security Update (cpuo. ↪.. OID:1.3.6.1.4.1.25623.1.0.170877 Version used: 2025-09-09T05:38:49Z
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-2024-5535 cve: CVE-2024-6119 cve: CVE-2024-21230 cve: CVE-2024-7264 cve: CVE-2024-21196
... continues on next page ...

...continued from previous page ...	
cve:	CVE-2024-21194
cve:	CVE-2024-21199
cve:	CVE-2024-21218
cve:	CVE-2024-21236
cve:	CVE-2024-21239
cve:	CVE-2024-21198
cve:	CVE-2024-21219
cve:	CVE-2024-21203
cve:	CVE-2024-21197
cve:	CVE-2024-21201
cve:	CVE-2024-21241
cve:	CVE-2024-21193
cve:	CVE-2024-21213
cve:	CVE-2024-21231
cve:	CVE-2024-21237
url:	https://www.oracle.com/security-alerts/cpuoct2024.html#AppendixMSQL
advisory-id:	cpuoct2024
cert-bund:	WID-SEC-2026-0180
cert-bund:	WID-SEC-2025-2838
cert-bund:	WID-SEC-2025-2836
cert-bund:	WID-SEC-2025-1560
cert-bund:	WID-SEC-2025-0823
cert-bund:	WID-SEC-2025-0814
cert-bund:	WID-SEC-2025-0612
cert-bund:	WID-SEC-2025-0225
cert-bund:	WID-SEC-2025-0166
cert-bund:	WID-SEC-2025-0148
cert-bund:	WID-SEC-2025-0143
cert-bund:	WID-SEC-2025-0001
cert-bund:	WID-SEC-2024-3674
cert-bund:	WID-SEC-2024-3412
cert-bund:	WID-SEC-2024-3201
cert-bund:	WID-SEC-2024-3196
cert-bund:	WID-SEC-2024-3192
cert-bund:	WID-SEC-2024-3188
cert-bund:	WID-SEC-2024-2112
cert-bund:	WID-SEC-2024-2040
cert-bund:	WID-SEC-2024-1736
cert-bund:	WID-SEC-2024-1469
dfn-cert:	DFN-CERT-2026-0015
dfn-cert:	DFN-CERT-2025-3495
dfn-cert:	DFN-CERT-2025-3494
dfn-cert:	DFN-CERT-2025-3493
dfn-cert:	DFN-CERT-2025-3492
dfn-cert:	DFN-CERT-2025-3491
dfn-cert:	DFN-CERT-2025-3324
dfn-cert:	DFN-CERT-2025-1659
...continues on next page ...	

...continued from previous page ...

```

dfn-cert: DFN-CERT-2025-1474
dfn-cert: DFN-CERT-2025-1454
dfn-cert: DFN-CERT-2025-0975
dfn-cert: DFN-CERT-2025-0854
dfn-cert: DFN-CERT-2025-0474
dfn-cert: DFN-CERT-2025-0446
dfn-cert: DFN-CERT-2025-0179
dfn-cert: DFN-CERT-2025-0175
dfn-cert: DFN-CERT-2025-0170
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2024-3300
dfn-cert: DFN-CERT-2024-3152
dfn-cert: DFN-CERT-2024-3013
dfn-cert: DFN-CERT-2024-2884
dfn-cert: DFN-CERT-2024-2783
dfn-cert: DFN-CERT-2024-2734
dfn-cert: DFN-CERT-2024-2732
dfn-cert: DFN-CERT-2024-2381
dfn-cert: DFN-CERT-2024-2322
dfn-cert: DFN-CERT-2024-2285
dfn-cert: DFN-CERT-2024-2168
dfn-cert: DFN-CERT-2024-2025
dfn-cert: DFN-CERT-2024-1978
dfn-cert: DFN-CERT-2024-1968
dfn-cert: DFN-CERT-2024-1967
dfn-cert: DFN-CERT-2024-1681

```

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.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 5.5.20

Fixed version: Apply the patch

Installation

path / port: 3306/tcp

... continues on next page ...

...continued from previous page ...
Impact 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: 2025-09-09T05:38:49Z
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-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: 7.2) 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.	
Quality of Detection (QoD): 80%	
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: 2025-09-09T05:38:49Z	
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-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 Unspecified Vulnerability-03 (Sep 2016) - 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.
Quality of Detection (QoD): 80%
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 (Sep 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.809300 Version used: 2025-09-09T05:38:49Z
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 ... continues on next page ...

...continued from previous page ...
url: http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html

High (CVSS: 7.2) NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpuja2016) - 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.
Quality of Detection (QoD): 80%
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 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 (cpuja20.↵.. OID:1.3.6.1.4.1.25623.1.0.806876 Version used: 2025-09-09T05:38:49Z
Product Detection Result ... continues on next page ...

...continued from previous page ...

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: WID-SEC-2024-1482
 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
 dfn-cert: DFN-CERT-2016-0104

High (CVSS: 7.2)

NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-06 (Oct 2015) - Windows

... continues on next page ...

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
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 (Oct 2015) - Windows OID:1.3.6.1.4.1.25623.1.0.805769 Version used: 2025-09-09T05:38:49Z
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-2015-4879 cve: CVE-2015-4819
... continues on next page ...

...continued from previous page ...
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: WID-SEC-2024-1483
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
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: 7.1)

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)

Summary

Oracle MySQL is prone to an unspecified vulnerability.

Quality of Detection (QoD): 80%

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:

... continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z
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-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 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: 7.1)

NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpu-jan2019) - 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.
Quality of Detection (QoD): 80%
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 Version used: 2025-09-09T05:38:49Z
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-2019-2534 cve: CVE-2019-2529
... continues on next page ...

...continued from previous page ...

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-2025-2349
cert-bund: WID-SEC-2025-1212
cert-bund: WID-SEC-2023-3083
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
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

...continues on next page ...

...continued from previous page ...

```

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: 7.0)

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.

Quality of Detection (QoD): 80%

... 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 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 Version used: 2025-09-09T05:38:49Z
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-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
...continues on next page ...

...continued from previous page ...

```

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

```

[\[return to 192.168.1.207 \]](#)**2.1.12 High 9200/tcp**

High (CVSS: 8.8)
 NVT: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Windows

Summary

Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

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

... continues on next page ...

...continued from previous page ...	
The <code>_cluster/settings</code> API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.113276 Version used: 2025-09-03T08:26:15Z	
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-2025-2802 dfn-cert: DFN-CERT-2020-1653	

[\[return to 192.168.1.207 \]](#)

2.1.13 High 22/tcp

High (CVSS: 7.8) NVT: OpenSSH < 7.4 Multiple Vulnerabilities (Jan 2017) - 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.	
Quality of Detection (QoD): 80%	
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 serial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.	
... continues on next page ...	

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 7.4 or later.
Affected Software/OS OpenSSH versions before 7.4 on Windows.
Vulnerability Insight Multiple flaws exist due to: <ul style="list-style-type: none"> - 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.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH < 7.4 Multiple Vulnerabilities (Jan 2017) - Windows OID:1.3.6.1.4.1.25623.1.0.810325 Version used: 2024-12-13T05:05:32Z
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=28652bca29046f62c7045e933e6b931de1d16737 cert-bund: WID-SEC-2023-1996
... continues on next page ...

...continued from previous page ...

```

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
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

```

High (CVSS: 7.5)

NVT: OpenSSH < 7.3 DoS 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 (DoS) and user enumeration vulnerabilities.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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 Update to version 7.3 or later.
Affected Software/OS OpenSSH versions before 7.3 on Windows.
Vulnerability Insight Multiple flaws exist due to: <ul style="list-style-type: none"> - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH < 7.3 DoS and User Enumeration Vulnerabilities - Windows OID:1.3.6.1.4.1.25623.1.0.809121 Version used: 2024-12-13T05:05:32Z
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
... continues on next page ...

...continued from previous page...

```

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-2023-1920
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
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

```

[\[return to 192.168.1.207 \]](#)**2.1.14 High 8181/tcp**

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

Product detection result

...continues on next page...

...continued from previous page ...
cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0. ↪802067)
Summary This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.
Quality of Detection (QoD): 98%
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) '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)
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
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 All 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 Checks previous collected cipher suites. Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031
... continues on next page ...

...continued from previous page ...
Version used: 2025-03-27T05:38:50Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
References cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel ↪ines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/ ↪TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch ↪eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes ↪tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↪-report-2014 url: https://sweet32.info cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1277 cert-bund: WID-SEC-2024-0209 cert-bund: WID-SEC-2024-0064 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 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
...continues on next page ...

...continued from previous page ...

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-2025-0041
 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
 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

...continues on next page ...

...continued from previous page ...

```

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

```

[\[return to 192.168.1.207 \]](#)

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

Summary

... continues on next page ...

...continued from previous page ...	
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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E7472616C2E636F6D,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	
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)	
Summary The remote server's SSL/TLS certificate has already expired.	
... continues on next page ...	

...continued from previous page...																																	
Quality of Detection (QoD): 99%																																	
<div><div>Vulnerability Detection Result</div><div>The certificate of the remote service expired on 2020-09-05 12:24:44.</div><div>Certificate details:</div><table><tr><td>fingerprint (SHA-1)</td><td> 701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315</td></tr><tr><td>fingerprint (SHA-256)</td><td> C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E</td></tr><tr><td colspan="2">↪B135AD83CD7B01A5A5</td></tr><tr><td>issued by</td><td> 1.2.840.113549.1.9.1=#737570706F7274406465736B</td></tr><tr><td colspan="2">↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora</td></tr><tr><td colspan="2">↪tion,L=Pleasanton,ST=CA,C=US</td></tr><tr><td>public key algorithm</td><td> RSA</td></tr><tr><td>public key size (bits)</td><td> 1024</td></tr><tr><td>serial</td><td> 00F59CEF71E6DB72A5</td></tr><tr><td>signature algorithm</td><td> sha1WithRSAEncryption</td></tr><tr><td>subject</td><td> 1.2.840.113549.1.9.1=#737570706F7274406465736B</td></tr><tr><td colspan="2">↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora</td></tr><tr><td colspan="2">↪tion,L=Pleasanton,ST=CA,C=US</td></tr><tr><td>subject alternative names (SAN)</td><td> None</td></tr><tr><td>valid from</td><td> 2010-09-08 12:24:44 UTC</td></tr><tr><td>valid until</td><td> 2020-09-05 12:24:44 UTC</td></tr></table></div>		fingerprint (SHA-1)	701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315	fingerprint (SHA-256)	C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E	↪B135AD83CD7B01A5A5		issued by	1.2.840.113549.1.9.1=#737570706F7274406465736B	↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora		↪tion,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=#737570706F7274406465736B	↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora		↪tion,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
fingerprint (SHA-1)	701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315																																
fingerprint (SHA-256)	C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E																																
↪B135AD83CD7B01A5A5																																	
issued by	1.2.840.113549.1.9.1=#737570706F7274406465736B																																
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora																																	
↪tion,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=#737570706F7274406465736B																																
↪746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corpora																																	
↪tion,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																																
<div><div>Solution:</div><div>Solution type: Mitigation</div><div>Replace the SSL/TLS certificate by a new one.</div></div>																																	
<div><div>Vulnerability Insight</div><div>This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.</div></div>																																	
<div><div>Vulnerability Detection Method</div><div>Details: SSL/TLS: Certificate Expired</div><div>OID:1.3.6.1.4.1.25623.1.0.103955</div><div>Version used: 2024-06-14T05:05:48Z</div></div>																																	
<div><div>Product Detection Result</div><div>Product: cpe:/a:ietf:transport_layer_security</div><div>Method: SSL/TLS: Collect and Report Certificate Details</div><div>OID: 1.3.6.1.4.1.25623.1.0.103692)</div></div>																																	
Medium (CVSS: 4.3)																																	
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection																																	
Product detection result																																	
... continues on next page ...																																	

...continued from previous page ...
cpe:/a:ietf:transport_layer_security:1.1 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
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 Checks 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: 2025-04-30T05:39:51Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security:1.1

Method: SSL/TLS: Version Detection

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

cve: CVE-2011-3389

cve: CVE-2015-0204

cve: CVE-2023-41928

cve: CVE-2024-41270

cve: CVE-2025-3200

url: <https://ssl-config.mozilla.org>url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.htmlurl: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.htmlurl: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>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://certvde.com/en/advisories/VDE-2025-031/>url: <https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc>url: <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>

cert-bund: WID-SEC-2026-0180

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

... continues on next page ...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...

```

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
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.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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 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 crypto- graphically 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 certifi- cates 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).
Quality of Detection (QoD): 80%
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. Please see the references for more resources supporting you with this task. - 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.
Affected Software/OS All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.
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 Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2025-03-27T05:38:50Z
References url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/↪TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch ... continues on next page ...

...continued from previous page ...
↪eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes ↪tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↪-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile

[[return to 192.168.1.207](#)]

2.1.16 Medium 3389/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Report Weak Cipher Suites
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0. ↪802067)
Summary This routine reports all weak SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
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
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
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.
Affected Software/OS All services providing an encrypted communication using weak SSL/TLS cipher suites.
... continues on next page ...

...continued from previous page ...

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

Checks previous collected cipher suites.

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.

Details: SSL/TLS: Report Weak Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.103440

Version used: 2025-03-27T05:38:50Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security

Method: SSL/TLS: Report Supported Cipher Suites

OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2013-2566

cve: CVE-2015-2808

cve: CVE-2015-4000

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuides/ines/TG02102/BSI-TR-02102-1.html>

url: https://www.bsi.bund.de/EN/Themen/oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>

url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html

url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

cert-bund: WID-SEC-2026-0180

cert-bund: CB-K21/0067

cert-bund: CB-K19/0812

cert-bund: CB-K17/1750

cert-bund: CB-K16/1593

cert-bund: CB-K16/1552

cert-bund: CB-K16/1102

...continues on next page ...

...continued from previous page ...

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-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692

...continues on next page ...

...continued from previous page ...

```

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

Product detection result

... continues on next page ...

...continued from previous page ...
cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can 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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
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 Checks 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: 2025-04-30T05:39:51Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security:1.0

Method: SSL/TLS: Version Detection

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

cve: CVE-2011-3389

cve: CVE-2015-0204

cve: CVE-2023-41928

cve: CVE-2024-41270

cve: CVE-2025-3200

url: <https://ssl-config.mozilla.org>url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.htmlurl: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.htmlurl: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>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://certvde.com/en/advisories/VDE-2025-031/>url: <https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc>url: <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>

cert-bund: WID-SEC-2026-0180

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

... continues on next page ...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...

```

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
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.

Quality of Detection (QoD): 80%

... continues on next page ...

...continued from previous page...

Vulnerability Detection Result

The following certificates are part of the certificate chain but using insecure ↪signature algorithms:

Subject: CN=vagrant-2008R2

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/>

[\[return to 192.168.1.207 \]](#)

2.1.17 Medium 8282/tcp

Medium (CVSS: 6.8) NVT: Apache Tomcat servlet/JSP container default files
Summary The Apache Tomcat servlet/JSP container has default files installed.
Quality of Detection (QoD): 99%
Vulnerability Detection Result The following default files were found : http://192.168.1.207:8282/examples/servlets/index.html http://192.168.1.207:8282/examples/jsp/snp/snoop.jsp http://192.168.1.207:8282/examples/jsp/index.html
Impact These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.
Solution: Solution type: Mitigation Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.
Vulnerability Insight Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.
Vulnerability Detection Method Details: Apache Tomcat servlet/JSP container default files OID:1.3.6.1.4.1.25623.1.0.12085 Version used: 2023-08-01T13:29:10Z

Medium (CVSS: 6.5) NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities - Windows
Summary Apache Tomcat is prone to multiple access bypass vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.0.50 Installation path / port: 8282/tcp
... continues on next page ...

...continued from previous page ...	
Impact	Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.
Solution: Solution type: VendorFix	Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.
Affected Software/OS	Apache Tomcat versions 9.0.0.M1 to 9.0.4 Apache Tomcat versions 8.5.0 to 8.5.27 Apache Tomcat versions 8.0.0.RC1 to 8.0.49 Apache Tomcat versions 7.0.0 to 7.0.84 on Windows.
Vulnerability Insight	Multiple flaws are due to: - The system does not properly enforce security constraints that defined by annotations of Servlets in certain cases, depending on the order that Servlets are loaded. - The URL pattern of " (the empty string) which exactly maps to the context root was not correctly handled when used as part of a security constraint definition.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit. ↪.. OID:1.3.6.1.4.1.25623.1.0.812784 Version used: 2025-09-17T05:39:26Z
References	cve: CVE-2018-1305 cve: CVE-2018-1304 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/103144 url: http://www.securityfocus.com/bid/103170 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html url: https://lists.apache.org/thread.html/b1d7e2425d6fd2cebed40d318f9365b4454607 ↪7e10949b01b1f8a0fb0%3Cannounce.tomcat.apache.org%3E cert-bund: WID-SEC-2024-1682 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K19/1121 cert-bund: CB-K19/0321 cert-bund: CB-K18/1007 cert-bund: CB-K18/1006 cert-bund: CB-K18/1005 cert-bund: CB-K18/0790
...continues on next page ...	

...continued from previous page ...

cert-bund: CB-K18/0420
 cert-bund: CB-K18/0349
 dfn-cert: DFN-CERT-2019-1627
 dfn-cert: DFN-CERT-2019-0772
 dfn-cert: DFN-CERT-2018-2165
 dfn-cert: DFN-CERT-2018-2142
 dfn-cert: DFN-CERT-2018-2125
 dfn-cert: DFN-CERT-2018-2103
 dfn-cert: DFN-CERT-2018-1753
 dfn-cert: DFN-CERT-2018-1407
 dfn-cert: DFN-CERT-2018-1274
 dfn-cert: DFN-CERT-2018-1253
 dfn-cert: DFN-CERT-2018-1038
 dfn-cert: DFN-CERT-2018-0922
 dfn-cert: DFN-CERT-2018-0733
 dfn-cert: DFN-CERT-2018-0455
 dfn-cert: DFN-CERT-2018-0378

Medium (CVSS: 6.4)

NVT: Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)

Summary

Apache Tomcat is prone to an authentication bypass vulnerability.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Installed version: 8.0.33

Fixed version: 9.0.96

Installation

path / port: 8282/tcp

Solution:**Solution type:** VendorFix

Update to version 9.0.96, 10.1.31, 11.0.0 or later.

Affected Software/OS

Apache Tomcat versions prior to 9.0.96, 10.0.x through 10.1.30 and 11.0.0-M1 through 11.0.0-M26.

... continues on next page ...

...continued from previous page ...
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.
Vulnerability Insight If Tomcat was configured to use a custom Jakarta Authentication (formerly JASPIC) ServerAuth-Context component which may throw an exception during the authentication process without explicitly setting an HTTP status to indicate failure, the authentication may not have failed, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows OID:1.3.6.1.4.1.25623.1.0.153463 Version used: 2024-12-19T05:05:34Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2024-52316 url: https://lists.apache.org/thread/lopz1qh91jj9n334g02om08sbysdb928 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.31 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.96 cert-bund: WID-SEC-2025-0521 cert-bund: WID-SEC-2024-3684 cert-bund: WID-SEC-2024-3486 dfn-cert: DFN-CERT-2025-2285 dfn-cert: DFN-CERT-2025-2098 dfn-cert: DFN-CERT-2025-0890 dfn-cert: DFN-CERT-2025-0146 dfn-cert: DFN-CERT-2025-0134 dfn-cert: DFN-CERT-2024-3156 dfn-cert: DFN-CERT-2024-3077
Medium (CVSS: 6.4) NVT: Apache Axis2 <= 1.6.2 Multiple Vulnerabilities
Summary Apache Axis2 is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 1.6.0 Fixed version: None Installation path / port: /axis2
Impact Successfully exploiting these issues allows attackers to: - CVE-2012-5785: perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks - CVE-2012-4418: may allow unauthenticated attackers to construct specially crafted messages that can be successfully verified and contain arbitrary content. This may aid in further attacks - CVE-2012-5351: allows remote attackers to forge messages and bypass authentication
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 The issue affects versions up to 1.6.2.
Vulnerability Insight The following flaws exist: - CVE-2012-5785: a security bypass vulnerability because the application fails to properly validate SSL certificates from the server - CVE-2012-4418: a security vulnerability involving XML signature wrapping - CVE-2012-5351: a SAML assertion that lacks a Signature element, aka a 'Signature exclusion attack'
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Axis2 <= 1.6.2 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.111004 Version used: 2025-01-17T15:39:18Z
References cve: CVE-2012-5785 cve: CVE-2012-4418 cve: CVE-2012-5351 url: https://issues.apache.org/jira/browse/AXIS2C-1607 url: http://www.securityfocus.com/bid/56408
... continues on next page ...

...continued from previous page ...
url: http://www.securityfocus.com/bid/55508

Medium (CVSS: 5.0) NVT: Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows
--

Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)

Summary Apache Tomcat is prone to a CGI security constraint bypass vulnerability.

Quality of Detection (QoD): 80%
--

Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.105 Installation path / port: 8282/tcp

Solution: Solution type: VendorFix Update to version 9.0.105, 10.1.41, 11.0.7 or later.

Affected Software/OS Apache Tomcat version 9.0.104 and prior, 10.x through 10.1.40 and 11.0.0-M1 through 11.0.6. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
--

Vulnerability Insight When running on a case insensitive file system with security constraints configured for the <code>pathInfo</code> component of a URL that mapped to the CGI servlet, it is possible to bypass those security constraints with a specially crafted URL.
--

Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows OID:1.3.6.1.4.1.25623.1.0.154591 Version used: 2025-05-30T15:42:19Z
--

Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2025-46701 url: https://lists.apache.org/thread/xhqqk9w5q45srcdqhogdk04lhdscv30j cert-bund: WID-SEC-2025-1850 cert-bund: WID-SEC-2025-1365 cert-bund: WID-SEC-2025-1165 dfn-cert: DFN-CERT-2026-0452 dfn-cert: DFN-CERT-2026-0451 dfn-cert: DFN-CERT-2025-2285 dfn-cert: DFN-CERT-2025-2098 dfn-cert: DFN-CERT-2025-1991 dfn-cert: DFN-CERT-2025-1905 dfn-cert: DFN-CERT-2025-1780 dfn-cert: DFN-CERT-2025-1384

Medium (CVSS: 5.0) NVT: Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.5.99 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 8.5.99, 9.0.86, 10.1.19, 11.0.0-M17 or later.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
<p>Apache Tomcat versions prior to 8.5.99, 9.0.0-M1 through 9.0.85, 10.x through 10.1.18 and 11.0.0-M1 through 11.0.0-M16.</p> <p>Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 8.5.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.</p>
<p>Vulnerability Insight</p> <p>The following flaws exist:</p> <ul style="list-style-type: none"> - CVE-2024-23672: WebSocket DoS with incomplete closing handshake - CVE-2024-24549: HTTP/2 header handling DoS
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.114428</p> <p>Version used: 2024-12-19T05:05:34Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:apache:tomcat:8.0.33</p> <p>Method: Apache Tomcat Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References</p> <p>cve: CVE-2024-23672</p> <p>cve: CVE-2024-24549</p> <p>url: https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f</p> <p>url: https://lists.apache.org/thread/4c50rmomhbbsdgmjsgwlb51xdwfdcvjg</p> <p>url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M1</p> <p>↪7</p> <p>url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.19</p> <p>url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.86</p> <p>url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.99</p> <p>url: https://nowotarski.info/http2-continuation-flood/</p> <p>url: https://nowotarski.info/http2-continuation-flood-technical-details/</p> <p>cert-bund: WID-SEC-2024-3663</p> <p>cert-bund: WID-SEC-2024-3508</p> <p>cert-bund: WID-SEC-2024-3377</p> <p>cert-bund: WID-SEC-2024-3220</p> <p>cert-bund: WID-SEC-2024-3219</p> <p>cert-bund: WID-SEC-2024-3196</p> <p>cert-bund: WID-SEC-2024-3195</p> <p>cert-bund: WID-SEC-2024-3191</p> <p>cert-bund: WID-SEC-2024-1656</p> <p>cert-bund: WID-SEC-2024-1642</p> <p>cert-bund: WID-SEC-2024-1638</p>
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2024-1622 cert-bund: WID-SEC-2024-1238 cert-bund: WID-SEC-2024-1214 cert-bund: WID-SEC-2024-1210 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0630 dfn-cert: DFN-CERT-2025-1517 dfn-cert: DFN-CERT-2024-3096 dfn-cert: DFN-CERT-2024-3078 dfn-cert: DFN-CERT-2024-2743 dfn-cert: DFN-CERT-2024-1846 dfn-cert: DFN-CERT-2024-1372 dfn-cert: DFN-CERT-2024-1235 dfn-cert: DFN-CERT-2024-1036 dfn-cert: DFN-CERT-2024-1011 dfn-cert: DFN-CERT-2024-0723 dfn-cert: DFN-CERT-2024-0722 dfn-cert: DFN-CERT-2024-0697

Medium (CVSS: 5.0) NVT: Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 9.0.98 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 9.0.98, 10.1.34, 11.0.2 or later. Vendor note: Users running Tomcat on a case insensitive file system with the default servlet write enabled (readonly initialisation parameter set to the non-default value of false) may need additional configuration to fully mitigate CVE-2024-50379 depending on which version of Java they are using with Tomcat:
... continues on next page ...

<p>...continued from previous page ...</p> <ul style="list-style-type: none"> - running on Java 8 or Java 11: the system property sun.io.useCanonCaches must be explicitly set to false (it defaults to true) - running on Java 17: the system property sun.io.useCanonCaches, if set, must be set to false (it defaults to false) - running on Java 21 onwards: no further configuration is required (the system property and the problematic cache have been removed)
<p>Affected Software/OS</p> <p>Apache Tomcat versions prior to 9.0.98, 10.x prior to 10.1.34 and 11.x prior to 11.0.2.</p> <p>Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.</p>
<p>Vulnerability Insight</p> <p>The following flaws exist:</p> <ul style="list-style-type: none"> - CVE-2024-50379: Remote code execution (RCE) via write-enabled default servlet - CVE-2024-54677: Denial of service (DoS) in examples web application - CVE-2024-56337: RCE via write-enabled default servlet - CVE-2024-50379 mitigation was incomplete
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.114890</p> <p>Version used: 2024-12-24T05:05:31Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:apache:tomcat:8.0.33</p> <p>Method: Apache Tomcat Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References</p> <p>cve: CVE-2024-50379</p> <p>cve: CVE-2024-54677</p> <p>cve: CVE-2024-56337</p> <p>url: https://lists.apache.org/thread/y6lj6q1xnp822g6ro70tn19sgtjmr80r</p> <p>url: https://lists.apache.org/thread/tdtbbxpg5trdwc2wnopcth9ccvdf tq2n</p> <p>url: https://lists.apache.org/thread/b2b9qrgjr z1kvo4ym8y2wkfdvwoq6qbp</p> <p>url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2</p> <p>url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34</p> <p>url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98</p> <p>cert-bund: WID-SEC-2025-0823</p> <p>cert-bund: WID-SEC-2025-0819</p> <p>cert-bund: WID-SEC-2025-0818</p>
<p>... continues on next page ...</p>

...continued from previous page ...
cert-bund: WID-SEC-2025-0808
cert-bund: WID-SEC-2025-0719
cert-bund: WID-SEC-2025-0148
cert-bund: WID-SEC-2024-3744
cert-bund: WID-SEC-2024-3722
dfn-cert: DFN-CERT-2025-2285
dfn-cert: DFN-CERT-2025-2098
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1923
dfn-cert: DFN-CERT-2025-1181
dfn-cert: DFN-CERT-2025-0974
dfn-cert: DFN-CERT-2025-0890
dfn-cert: DFN-CERT-2025-0888
dfn-cert: DFN-CERT-2025-0766
dfn-cert: DFN-CERT-2025-0528
dfn-cert: DFN-CERT-2025-0509
dfn-cert: DFN-CERT-2025-0444
dfn-cert: DFN-CERT-2025-0146
dfn-cert: DFN-CERT-2025-0138
dfn-cert: DFN-CERT-2025-0134
dfn-cert: DFN-CERT-2025-0036
dfn-cert: DFN-CERT-2024-3364

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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following URLs requires Basic Authentication (URL:realm name): http://192.168.1.207:8282/host-manager/html:"Tomcat Host Manager Application" http://192.168.1.207:8282/manager/html:"Tomcat Manager Application" http://192.168.1.207:8282/manager/status:"Tomcat Manager Application"
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
... continues on next page ...

...continued from previous page ...
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: 2023-09-07T05:05:21Z
References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_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: 4.3) NVT: Apache Tomcat Open Redirect Vulnerability - Windows
Summary When the default servlet in Apache Tomcat returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.5.34 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 7.0.91, 8.5.34, 9.0.12 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Open Redirect Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.141569 Version used: 2024-02-15T05:05:40Z
References cve: CVE-2018-11784 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html cert-bund: WID-SEC-2025-1212 cert-bund: WID-SEC-2024-1682 cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2023-0531 cert-bund: WID-SEC-2023-0460 cert-bund: CB-K20/0029 cert-bund: CB-K19/1121 cert-bund: CB-K19/0907 cert-bund: CB-K19/0616 cert-bund: CB-K19/0320 cert-bund: CB-K19/0050 cert-bund: CB-K18/0963 dfn-cert: DFN-CERT-2019-2710 dfn-cert: DFN-CERT-2019-2159 dfn-cert: DFN-CERT-2019-1562 dfn-cert: DFN-CERT-2019-1237 dfn-cert: DFN-CERT-2019-0771 dfn-cert: DFN-CERT-2019-0147 dfn-cert: DFN-CERT-2019-0104 dfn-cert: DFN-CERT-2018-2435 dfn-cert: DFN-CERT-2018-2165 dfn-cert: DFN-CERT-2018-2142 dfn-cert: DFN-CERT-2018-2000
Medium (CVSS: 4.3) NVT: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows
Product detection result cpe:/a:apache:tomcat:8.0.33 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
... continues on next page ...

...continued from previous page ...
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 8.0.33 Fixed version: 8.5.86 Installation path / port: 8282/tcp
Solution: Solution type: VendorFix Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.
Affected Software/OS Apache Tomcat versions through 8.5.85, 9.0.0-M1 through 9.0.71, 10.x through 10.1.5 and 11.0.0-M1 through 11.0.0-M2.
Vulnerability Insight When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Tomcat did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows OID:1.3.6.1.4.1.25623.1.0.104654 Version used: 2024-06-07T05:05:42Z
Product Detection Result Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2023-28708 url: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.6 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.72 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86 cert-bund: WID-SEC-2024-1238
... continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2024-0528
cert-bund:	WID-SEC-2023-2674
cert-bund:	WID-SEC-2023-1812
cert-bund:	WID-SEC-2023-1808
cert-bund:	WID-SEC-2023-1784
cert-bund:	WID-SEC-2023-1783
cert-bund:	WID-SEC-2023-1782
cert-bund:	WID-SEC-2023-1424
cert-bund:	WID-SEC-2023-1021
cert-bund:	WID-SEC-2023-1017
cert-bund:	WID-SEC-2023-0717
dfn-cert:	DFN-CERT-2025-1517
dfn-cert:	DFN-CERT-2024-3078
dfn-cert:	DFN-CERT-2023-2778
dfn-cert:	DFN-CERT-2023-2545
dfn-cert:	DFN-CERT-2023-2054
dfn-cert:	DFN-CERT-2023-0772
dfn-cert:	DFN-CERT-2023-0763
dfn-cert:	DFN-CERT-2023-0640

[\[return to 192.168.1.207 \]](#)

2.1.18 Medium 8022/tcp

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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.1.207:8022/configurations.do:j_password
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: Solution type: Workaround
... continues on next page ...

...continued from previous page ...
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: 2023-09-07T05:05:21Z
References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html

[\[return to 192.168.1.207 \]](#)

2.1.19 Medium 4848/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)
Summary The remote server's SSL/TLS certificate has already expired.
Quality of Detection (QoD): 99%
Vulnerability Detection Result The certificate of the remote service expired on 2023-05-13 05:33:38. Certificate details:
... continues on next page ...

...continued from previous page...	
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: 2024-06-14T05:05:48Z	
Product Detection Result	
Product: cpe:/a:ietf:transport_layer_security	
Method: SSL/TLS: Collect and Report Certificate Details	
OID: 1.3.6.1.4.1.25623.1.0.103692)	
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.	
Quality of Detection (QoD): 70%	
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	
... continues on next page ...	

... continued from previous page ...	
<pre> ↔----- TLSv1.0 10 TLSv1.1 10 TLSv1.2 10 </pre>	
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: 2024-09-27T05:05:23Z	
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/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 cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796	
... continues on next page ...	

...continued from previous page ...

```

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-2025-0933
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: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

cpe:/a:ietf:transport_layer_security

Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
 ↪623.1.0.103692)

Summary

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Quality of Detection (QoD): 99%**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

... continues on next page ...

...continued from previous page ...	
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: 2024-06-14T05:05:48Z	
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)	
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	
Product detection result cpe:/a:ietf:transport_layer_security:1.1 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)	
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	
Quality of Detection (QoD): 98%	
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 ... continues on next page ...	

...continued from previous page ...
<p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS</p> <ul style="list-style-type: none"> - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
<p>Vulnerability Insight</p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - 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)
<p>Vulnerability Detection Method</p> <p>Checks the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2025-04-30T05:39:51Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:transport_layer_security:1.1</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p>References</p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>cve: CVE-2023-41928</p> <p>cve: CVE-2024-41270</p> <p>cve: CVE-2025-3200</p> <p>url: https://ssl-config.mozilla.org</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html</p> <p>url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/</p>
...continues on next page ...

...continued from previous page...

↪TLS-Protokoll/TLS-Protokoll_node.html
 url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch↪eRichtlinien/TR03116/BSI-TR-03116-4.html>
 url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes↪tstandard_BSI_TLS_Version_2_4.html
 url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>
 url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters↪-report-2014>
 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://certvde.com/en/advisories/VDE-2025-031/>
 url: <https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc>
 url: <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>
 cert-bund: WID-SEC-2026-0180
 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

...continues on next page...

...continued from previous page ...

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
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

...continues on next page ...

...continued from previous page ...	
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: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
Summary The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
Quality of Detection (QoD): 80%
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. Please see the references for more resources supporting you with this task. - 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.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.
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: 2025-03-27T05:38:50Z
References url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel↪ines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/↪TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch↪eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes↪tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters↪-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile

[[return to 192.168.1.207](#)]

2.1.20 Medium 3306/tcp

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)
... continues on next page ...

...continued from previous page ...
Summary Oracle MySQL Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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.
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: 2025-09-09T05:38:49Z
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-2012-5612 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: 6.8) NVT: Oracle MySQL Server Multiple Vulnerabilities - 02 - (Nov 2012) - 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.
Quality of Detection (QoD): 80%
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 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 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803112 Version used: 2025-09-09T05:38:49Z
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-2012-3180 cve: CVE-2012-3177 ... continues on next page ...

...continued from previous page ...
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 <= 5.1.65 / 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.5.28 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. ↵..
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.117201 Version used: 2025-09-09T05:38:49Z
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-2012-5060 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 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.
Quality of Detection (QoD): 80%
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.
Affected Software/OS Oracle MySQL Server 5.5.x through 5.5.23.
... 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.x <= 5.5.23 Security Update (cpujul2012) - Windows OID:1.3.6.1.4.1.25623.1.0.117267 Version used: 2025-09-09T05:38:49Z
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-2012-1735 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: 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...
Affected Software/OS MySQL version 5.1.x before 5.1.62 and 5.5.x before 5.5.22.
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: 2025-09-09T05:38:49Z
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#AppendixMySQL 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: 6.7) 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)
Summary ... continues on next page ...

...continued from previous page ...
Oracle MySQL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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 cve: CVE-2017-3244
... continues on next page ...

...continued from previous page ...
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: 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 5.5.20

Fixed version: 5.5.29

Installation

path / port: 3306/tcp

... continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z	
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-2013-1531 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 <= 5.5.50 / 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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20	
... continues on next page ...	

...continued from previous page...	
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 5.5.50 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: 2025-09-09T05:38:49Z	
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-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 <= 5.7.32 / 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.33 Installation 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: 2025-09-09T05:38:49Z
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-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-2024-0794
... continues on next page ...

...continued from previous page ...

```

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
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: 6.5)

NVT: Oracle MySQL Server <= 8.0.41, 8.1 <= 8.4.4, 9.0 <= 9.2.0 Security Update (cpuapr2025)- Windows

...continues on next page ...

...continued from previous page ...	
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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.42 Installation path / port: 3306/tcp	
Solution: Solution type: VendorFix Update to version 8.0.42, 8.4.5, 9.3.0 or later.	
Affected Software/OS Oracle MySQL Server version 8.0.41 and prior, 8.1 through 8.4.4 and 9.0 through 9.2.0.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.41, 8.1 <= 8.4.4, 9.0 <= 9.2.0 Security Update (cpua.↪.. OID:1.3.6.1.4.1.25623.1.0.171442 Version used: 2025-09-09T05:38:49Z	
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-2025-21577 cve: CVE-2025-30682 cve: CVE-2025-30687 cve: CVE-2025-30688 cve: CVE-2025-21574 cve: CVE-2025-21575 cve: CVE-2025-30693 cve: CVE-2025-30695	
... continues on next page ...	

...continued from previous page ...	
cve:	CVE-2025-30715
cve:	CVE-2025-21584
cve:	CVE-2025-21580
cve:	CVE-2025-21581
cve:	CVE-2025-21585
cve:	CVE-2025-30689
cve:	CVE-2025-21579
cve:	CVE-2025-30696
cve:	CVE-2025-30705
cve:	CVE-2025-30683
cve:	CVE-2025-30684
cve:	CVE-2025-30685
cve:	CVE-2025-30699
cve:	CVE-2025-30704
cve:	CVE-2024-13176
cve:	CVE-2024-9143
cve:	CVE-2025-30721
cve:	CVE-2025-30703
cve:	CVE-2025-30681
url:	https://www.oracle.com/security-alerts/cpuapr2025.html#AppendixMSQL
advisory-id:	cpuapr2025
cert-bund:	WID-SEC-2025-2364
cert-bund:	WID-SEC-2025-1850
cert-bund:	WID-SEC-2025-1572
cert-bund:	WID-SEC-2025-1568
cert-bund:	WID-SEC-2025-1566
cert-bund:	WID-SEC-2025-1564
cert-bund:	WID-SEC-2025-1560
cert-bund:	WID-SEC-2025-1257
cert-bund:	WID-SEC-2025-1035
cert-bund:	WID-SEC-2025-0828
cert-bund:	WID-SEC-2025-0818
cert-bund:	WID-SEC-2025-0813
cert-bund:	WID-SEC-2025-0148
cert-bund:	WID-SEC-2025-0131
cert-bund:	WID-SEC-2024-3230
dfn-cert:	DFN-CERT-2026-0037
dfn-cert:	DFN-CERT-2025-3583
dfn-cert:	DFN-CERT-2025-3324
dfn-cert:	DFN-CERT-2025-2944
dfn-cert:	DFN-CERT-2025-2602
dfn-cert:	DFN-CERT-2025-2523
dfn-cert:	DFN-CERT-2025-1905
dfn-cert:	DFN-CERT-2025-1903
dfn-cert:	DFN-CERT-2025-1901
dfn-cert:	DFN-CERT-2025-1898
dfn-cert:	DFN-CERT-2025-1648
...continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2025-1611
dfn-cert: DFN-CERT-2025-1470
dfn-cert: DFN-CERT-2025-1424
dfn-cert: DFN-CERT-2025-1304
dfn-cert: DFN-CERT-2025-0993
dfn-cert: DFN-CERT-2025-0981
dfn-cert: DFN-CERT-2025-0974
dfn-cert: DFN-CERT-2025-0973
dfn-cert: DFN-CERT-2025-0564
dfn-cert: DFN-CERT-2025-0465
dfn-cert: DFN-CERT-2025-0354
dfn-cert: DFN-CERT-2025-0158
dfn-cert: DFN-CERT-2024-2884
dfn-cert: DFN-CERT-2024-2764

Medium (CVSS: 6.5) 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-2018-2767 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
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)
... continues on next page ...

...continued from previous page ...
Summary Oracle MySQL is prone to an unspecified vulnerability.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

```
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.

Quality of Detection (QoD): 80%**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'

... 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 Security Updates (oct2017-3236626) 04 - Windows

OID:1.3.6.1.4.1.25623.1.0.811991

Version used: 2025-09-09T05:38:49Z

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-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 <= 5.5.51 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.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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

<p>Medium (CVSS: 6.5) NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows</p>
<p>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)</p>
<p>Summary Oracle MySQL is prone to multiple denial of service (DoS) vulnerabilities.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Installed version: 5.5.20 Fixed version: Apply the patch Installation path / port: 3306/tcp</p>
<p>Impact Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.</p>
<p>Solution: Solution type: VendorFix Apply the patch from the referenced advisory.</p>
<p>Affected Software/OS Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows</p>
<p>Vulnerability Insight Multiple flaws exist due to: - An error in the 'Server: DDL' component. - Multiple errors in the 'Server: Optimizer' component.</p>
<p>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: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>... continues on next page ...</p>

...continued from previous page ...

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>
 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 Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpu-jul2019) - 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.

Quality of Detection (QoD): 80%

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

... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-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 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: 6.5) NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (cpuoct2019) - Windows
... continues on next page ...

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-2019-2974 cve: CVE-2019-2911 url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL advisory-id: cpuoct2019
...continues on next page ...

...continued from previous page ...

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
 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 Multiple Unspecified vulnerabilities-02 (Jul 2014) - 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.

Quality of Detection (QoD): 80%**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.

... continues on next page ...

...continued from previous page ...
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 (Jul 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804722 Version used: 2025-09-09T05:38:49Z
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-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_security_patches url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#AppendixMSQL 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 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 ... continues on next page ...

...continued from previous page ...
Oracle MySQL Server is prone to an unspecified denial of service vulnerability.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-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 <= 5.6.49 / 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.
... continues on next page ...

...continued from previous page ...
↔25623.1.0.100152)
Summary Oracle MySQL Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-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: WID-SEC-2026-0205 cert-bund: CB-K20/1066 cert-bund: CB-K20/1017
... continues on next page ...

...continued from previous page ...
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 <= 5.1.67 / 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)
Summary Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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. ... continues on next page ...

...continued from previous page ...
↔... OID:1.3.6.1.4.1.25623.1.0.117209 Version used: 2025-09-09T05:38:49Z
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 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...
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. 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: 2025-09-09T05:38:49Z
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-2013-2378 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.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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.
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: 2025-09-09T05:38:49Z
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-2013-2375 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
... continues on next page ...

...continued from previous page ...
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 <= 5.5.31 / 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.
Quality of Detection (QoD): 80%
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. ↵..
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.806878 Version used: 2025-09-09T05:38:49Z
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-2016-0502 url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL url: http://www.securityfocus.com/bid/81136 advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...	
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	
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: 2025-09-09T05:38:49Z	
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-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	
... continues on next page ...	

...continued from previous page ...
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: 6.5) NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 (May 2014) - 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.
Quality of Detection (QoD): 80%
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 5.5.36 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 (May 2014) - Windows ... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.804575 Version used: 2025-09-09T05:38:49Z
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-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: 6.4) NVT: Oracle MySQL Server Multiple Vulnerabilities - 04 - (Nov 2012) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: Apply the patch
... continues on next page ...

...continued from previous page ...
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 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803114 Version used: 2025-09-09T05:38:49Z
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-2012-3147 cve: CVE-2012-3149 cve: CVE-2012-3144 url: http://secunia.com/advisories/51008/ 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
... continues on next page ...

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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

<p>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</p>
<p>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)</p>
<p>Summary Oracle MySQL Server is prone to multiple unspecified vulnerabilities.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp</p>
<p>Impact Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.</p>
<p>Solution: Solution type: VendorFix Updates are available. Please see the references for more information.</p>
<p>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.</p>
<p>Vulnerability Insight Unspecified errors exist in the 'MySQL Server' component via unknown vectors.</p>
<p>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: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>... continues on next page ...</p>

...continued from previous page ...

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#AppendixMySQL>
 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: 5.9)

NVT: Oracle MySQL Backronym Vulnerability (Jun 2016) - 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 5.5.20

Fixed version: 5.7.3

Installation

path / port: 3306/tcp

Impact

... continues on next page ...

...continued from previous page ...
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 <code>--ssl</code> option.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Backronym Vulnerability (Jun 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.808063 Version used: 2025-09-09T05:38:49Z
Product Detection Result Product: <code>cpe:/a:mysql:mysql:5.5.20-log</code> 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

<p>Medium (CVSS: 5.9)</p> <p>NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Windows</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.5.20-log</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↪25623.1.0.100152)</p>
<p>Summary</p> <p>Oracle MySQL Server is prone to a unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.5.20</p> <p>Fixed version: 5.7.43</p> <p>Installation</p> <p>path / port: 3306/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 5.7.43, 8.0.34 or later.</p>
<p>Affected Software/OS</p> <p>Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Win. ↪..</p> <p>OID:1.3.6.1.4.1.25623.1.0.149981</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2023-22053</p> <p>url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL</p> <p>advisory-id: cpujul2023</p> <p>cert-bund: WID-SEC-2024-1248</p> <p>cert-bund: WID-SEC-2023-1794</p> <p>dfn-cert: DFN-CERT-2024-1188</p>
<p>... continues on next page ...</p>

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0593
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0454
dfn-cert: DFN-CERT-2023-1642

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.
Quality of Detection (QoD): 80%
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. ↪..
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.117194 Version used: 2025-09-09T05:38:49Z
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-2015-7744 url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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 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)
Summary Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-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 <= 5.6.43 / 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
<p>Installed version: 5.5.20 Fixed version: 5.6.44 Installation path / port: 3306/tcp</p>
<p>Solution: Solution type: VendorFix Update to version 5.6.44, 5.7.26, 8.0.16 or later.</p>
<p>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.</p>
<p>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.</p>
<p>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: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>References cve: CVE-2019-1559 cve: CVE-2019-2683 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-2026-0180 cert-bund: WID-SEC-2023-2946 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</p>
...continues on next page ...

...continued from previous page ...

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
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

<p>Medium (CVSS: 5.9)</p> <p>NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - Windows</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.5.20-log</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)</p>
<p>Summary</p> <p>Oracle MySQL Server is prone to multiple unspecified vulnerabilities.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.5.20</p> <p>Fixed version: See the referenced vendor advisory</p> <p>Installation</p> <p>path / port: 3306/tcp</p>
<p>Impact</p> <p>Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Updates are available. Please see the references for more information.</p>
<p>Affected Software/OS</p> <p>Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.</p>
<p>Vulnerability Insight</p> <p>Unspecified errors exist in the 'MySQL Server' component via unknown vectors.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (↵..</p> <p>OID:1.3.6.1.4.1.25623.1.0.807924</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>... continues on next page ...</p>

...continued from previous page ...

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
 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: 5.7)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Apr 2015) - 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Installed version: 5.5.20

... continues on next page ...

...continued from previous page ...	
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	
Checks if a vulnerable version is present on the target host.	
Details: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Apr 2015) - Windows	
OID:1.3.6.1.4.1.25623.1.0.805172	
Version used: 2025-09-09T05:38:49Z	
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-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: WID-SEC-2023-2068	
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	
... continues on next page ...	

...continued from previous page ...

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: 5.5)

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.

Quality of Detection (QoD): 80%**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 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

... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-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 <= 8.0.43, 8.1.x <= 8.4.7, 9.0.0 <= 9.4.0 Security Update (cpuoct2025) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.44
... continues on next page ...

...continued from previous page...	
Installation	
path / port:	3306/tcp
Solution:	
Solution type: VendorFix	
Update to version 8.0.44, 8.4.7, 9.4.1 or later.	
Affected Software/OS	
Oracle MySQL Server versions 8.0.43 and prior, 8.1.x through 8.4.6 and 9.0.0 through 9.4.0. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that all versions prior to 8.x and versions like 9.2.x in between are also affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.	
Vulnerability Detection Method	
Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.43, 8.1.x <= 8.4.7, 9.0.0 <= 9.4.0 Security Update (. ↔.. OID:1.3.6.1.4.1.25623.1.0.119199 Version used: 2025-10-24T05:39:31Z	
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-2025-53054 cve: CVE-2025-53053 cve: CVE-2025-53044 cve: CVE-2025-53045 cve: CVE-2025-53062 cve: CVE-2025-53069 cve: CVE-2025-53040 cve: CVE-2025-53042 url: https://www.oracle.com/security-alerts/cpuoct2025.html#AppendixMSQL advisory-id: cpuoct2025 cert-bund: WID-SEC-2025-2363 dfn-cert: DFN-CERT-2026-0409 dfn-cert: DFN-CERT-2025-3598 dfn-cert: DFN-CERT-2025-2945	

Medium (CVSS: 5.4) 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.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-2012-5611 cve: CVE-2013-0384 cve: CVE-2013-0389 cve: CVE-2013-0385 cve: CVE-2013-0375 cve: CVE-2012-1702
... continues on next page ...

...continued from previous page ...

```

cve: CVE-2013-0383
cve: CVE-2012-0572
cve: CVE-2012-0574
cve: CVE-2012-1705
cve: CVE-2012-4414
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMySQL
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: 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.

Quality of Detection (QoD): 80%**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 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: 2025-09-09T05:38:49Z
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-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)
... continues on next page ...

...continued from previous page ...
Summary Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.
Quality of Detection (QoD): 80%
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. ↪.. OID:1.3.6.1.4.1.25623.1.0.143735 Version used: 2025-09-09T05:38:49Z
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-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-2023-3081 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
... continues on next page ...

...continued from previous page ...	
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: 2025-09-09T05:38:49Z	
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-2019-2922 cve: CVE-2019-2923 cve: CVE-2019-2924 cve: CVE-2019-2910 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 (jul2017-3236622) 03 - 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 vulnerability.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

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 Security Updates (jul2017-3236622) 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.

Quality of Detection (QoD): 80%**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

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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.
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.811432</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2017-3651</p> <p>cve: CVE-2017-3653</p> <p>cve: CVE-2017-3652</p> <p>cve: CVE-2017-3635</p> <p>cve: CVE-2017-3648</p> <p>cve: CVE-2017-3641</p> <p>url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html</p> <p>↪#AppendixMSQL</p> <p>url: http://www.securityfocus.com/bid/99802</p> <p>url: http://www.securityfocus.com/bid/99810</p> <p>url: http://www.securityfocus.com/bid/99805</p> <p>url: http://www.securityfocus.com/bid/99730</p> <p>url: http://www.securityfocus.com/bid/99789</p> <p>url: http://www.securityfocus.com/bid/99767</p> <p>cert-bund: CB-K18/0224</p> <p>cert-bund: CB-K17/1870</p> <p>cert-bund: CB-K17/1732</p> <p>cert-bund: CB-K17/1604</p> <p>cert-bund: CB-K17/1453</p> <p>cert-bund: CB-K17/1401</p> <p>cert-bund: CB-K17/1298</p> <p>cert-bund: CB-K17/1239</p> <p>cert-bund: CB-K17/1205</p> <p>dfn-cert: DFN-CERT-2018-1276</p> <p>dfn-cert: DFN-CERT-2018-0242</p> <p>dfn-cert: DFN-CERT-2017-1956</p> <p>dfn-cert: DFN-CERT-2017-1806</p> <p>dfn-cert: DFN-CERT-2017-1675</p>
...continues on next page ...

...continued from previous page ...
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: 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.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-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-2024-1591
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1969
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-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2491
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 <= 8.0.39, 8.1 <= 8.4.1, 9.0 <= 9.0.1 Security Update (cpuoct2024) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.40 Installation path / port: 3306/tcp
Solution: Solution type: VendorFix Update to version 8.0.40, 8.4.2, 9.0.2 or later.
Affected Software/OS Oracle MySQL Server version 8.0.39 and prior, 8.1 through 8.4.1 and 9.0 through 9.0.1.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.39, 8.1 <= 8.4.1, 9.0 <= 9.0.1 Security Update (cpuo. ↵.. OID:1.3.6.1.4.1.25623.1.0.170873 Version used: 2025-09-09T05:38:49Z
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-2024-21238 url: https://www.oracle.com/security-alerts/cpuoct2024.html#AppendixMSQL advisory-id: cpuoct2024 cert-bund: WID-SEC-2024-3188 dfn-cert: DFN-CERT-2025-0446
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2024-2732

Medium (CVSS: 5.0)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 (Apr 2015) - 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.

Quality of Detection (QoD): 80%**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

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 (Apr 2015) - Windows

OID:1.3.6.1.4.1.25623.1.0.805171

Version used: 2025-09-09T05:38:49Z

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-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: WID-SEC-2023-2068 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: 5.0)

NVT: MySQL Unspecified vulnerabilities-03 (Jul 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
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 (Jul 2013) - Windows OID:1.3.6.1.4.1.25623.1.0.803725 Version used: 2025-09-09T05:38:49Z
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-2013-3801 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

<p>Medium (CVSS: 4.9)</p> <p>NVT: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.5.20-log</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)</p>
<p>Summary</p> <p>Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.5.20</p> <p>Fixed version: 5.7.34</p> <p>Installation</p> <p>path / port: 3306/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 5.7.34 or later.</p>
<p>Affected Software/OS</p> <p>Oracle MySQL Server version 5.7.33 and prior.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.145802</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2021-2154</p> <p>url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL</p> <p>advisory-id: cpuapr2021</p> <p>cert-bund: WID-SEC-2023-0065</p> <p>cert-bund: CB-K21/0421</p> <p>dfn-cert: DFN-CERT-2022-1241</p> <p>dfn-cert: DFN-CERT-2022-0933</p>
<p>... continues on next page ...</p>

...continued from previous page ...
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 <= 5.7.30 / 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.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-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 <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpu-jan2021) - 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.

Quality of Detection (QoD): 80%**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: 2025-09-09T05:38:49Z

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-2021-2060 cve: CVE-2021-2022 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 <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpu-jan2021) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.6.51 Installation path / port: 3306/tcp
Impact 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. ... 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 <= 5.6.50 / 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: 2025-09-09T05:38:49Z
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-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: 4.9) 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)
Summary Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.41 Installation path / port: 3306/tcp
Solution: Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-2023-21840 url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL advisory-id: cpujan2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0126 dfn-cert: DFN-CERT-2023-0105

Medium (CVSS: 4.9) NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpujul2023) - 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.
Quality of Detection (QoD): 80%
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, 8.0.33 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 (cpujul2023) - Win. ↔.. OID:1.3.6.1.4.1.25623.1.0.149979 Version used: 2025-09-09T05:38:49Z	
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-2023-22007 url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL advisory-id: cpujul2023 cert-bund: WID-SEC-2023-1794 dfn-cert: DFN-CERT-2024-1188 dfn-cert: DFN-CERT-2024-0593 dfn-cert: DFN-CERT-2024-0454 dfn-cert: DFN-CERT-2023-1642	

Medium (CVSS: 4.9) NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.31 Security Update (cpuoct2023) - 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.	
Quality of Detection (QoD): 80%	
... continues on next page ...	

...continued from previous page ...	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.43 Installation path / port: 3306/tcp	
Solution: Solution type: VendorFix Update to version 5.7.43, 8.0.32 or later.	
Affected Software/OS Oracle MySQL Server version 5.7.42 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 <= 5.7.42, 8.x <= 8.0.31 Security Update (cpuoct2023) - Win. ↔.. OID:1.3.6.1.4.1.25623.1.0.151212 Version used: 2025-09-09T05:38:49Z	
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-2023-22015 cve: CVE-2023-22026 url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL advisory-id: cpuoct2023 cert-bund: WID-SEC-2023-2690 dfn-cert: DFN-CERT-2023-2536	
Medium (CVSS: 4.9) NVT: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.31 Security Update (cpuoct2023) - 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 denial of service (DoS) vulnerability.	
... continues on next page ...	

...continued from previous page ...	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.44 Installation path / port: 3306/tcp	
Solution: Solution type: VendorFix Update to version 5.7.44, 8.0.32 or later.	
Affected Software/OS Oracle MySQL Server version 5.7.43 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 <= 5.7.43, 8.x <= 8.0.31 Security Update (cpuoct2023) - Win. ↔.. OID:1.3.6.1.4.1.25623.1.0.151216 Version used: 2025-09-09T05:38:49Z	
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-2023-22028 url: https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL advisory-id: cpuoct2023 cert-bund: WID-SEC-2023-2690 dfn-cert: DFN-CERT-2024-0108 dfn-cert: DFN-CERT-2023-2536	

Medium (CVSS: 4.9) NVT: Oracle MySQL Server <= 8.0.35 Security Update (cpuoct2024) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.36 Installation path / port: 3306/tcp
Solution: Solution type: VendorFix Update to version 8.0.36 or later.
Affected Software/OS Oracle MySQL Server version 8.0.35 and prior.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.35 Security Update (cpuoct2024) - Windows OID:1.3.6.1.4.1.25623.1.0.170867 Version used: 2025-09-09T05:38:49Z
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-2024-21200 url: https://www.oracle.com/security-alerts/cpuoct2024.html#AppendixMSQL advisory-id: cpuoct2024 cert-bund: WID-SEC-2024-3188 dfn-cert: DFN-CERT-2024-2732
Medium (CVSS: 4.9) NVT: Oracle MySQL Server <= 8.0.38, 8.1 <= 8.4.1, 9.0 <= 9.0.1 Security Update (cpuoct2024) - 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 Server is prone to a denial of service (DoS) vulnerability.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.39 Installation path / port: 3306/tcp	
Solution: Solution type: VendorFix Update to version 8.0.39, 8.4.2, 9.0.2 or later.	
Affected Software/OS Oracle MySQL Server version 8.0.38 and prior, 8.1 through 8.4.1 and 9.0 through 9.0.1.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.38, 8.1 <= 8.4.1, 9.0 <= 9.0.1 Security Update (cpuo. ↔.. OID:1.3.6.1.4.1.25623.1.0.170869 Version used: 2025-09-09T05:38:49Z	
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-2024-21207 url: https://www.oracle.com/security-alerts/cpuoct2024.html#AppendixMSQL advisory-id: cpuoct2024 cert-bund: WID-SEC-2024-3188 dfn-cert: DFN-CERT-2024-2732	

Medium (CVSS: 4.9) NVT: Oracle MySQL Server Component 'Replication' Unspecified vulnerability (Oct 2013) - Windows
... continues on next page ...

...continued from previous page ...	
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.	
Quality of Detection (QoD): 80%	
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.↪.. OID:1.3.6.1.4.1.25623.1.0.804034 Version used: 2025-09-09T05:38:49Z	
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	
...continues on next page ...	

...continued from previous page ...

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 Security Update (cpujul2018 - 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 a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%**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

... continues on next page ...

...continued from previous page ...
<p>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: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>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 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</p>

<p>Medium (CVSS: 4.6) NVT: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) - Windows</p>
<p>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)</p>
<p>Summary Oracle MySQL Server is prone to an unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.5.30 Installation path / port: 3306/tcp</p>
...continues on next page ...

...continued from previous page ...
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) . ↔.. OID:1.3.6.1.4.1.25623.1.0.117213 Version used: 2025-09-09T05:38:49Z
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-2013-1523 url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL advisory-id: cpuapr2013 dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.4) NVT: Oracle MySQL Server <= 8.0.39, 8.1 <= 8.4.0 Security Update (cpuoct2024) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 8.0.40 Installation path / port: 3306/tcp
... continues on next page ...

...continued from previous page ...	
Solution: Solution type: VendorFix Update to version 8.0.40, 8.4.1 or later.	
Affected Software/OS Oracle MySQL Server version 8.0.39 and prior and 8.1 through 8.4.0.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 8.0.39, 8.1 <= 8.4.0 Security Update (cpuoct2024) - Wind. ↔.. OID:1.3.6.1.4.1.25623.1.0.170871 Version used: 2025-09-09T05:38:49Z	
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-2024-21212 url: https://www.oracle.com/security-alerts/cpuoct2024.html#AppendixMSQL advisory-id: cpuoct2024 cert-bund: WID-SEC-2024-3188 dfn-cert: DFN-CERT-2025-0446 dfn-cert: DFN-CERT-2024-2732	

Medium (CVSS: 4.4) NVT: Oracle Mysq! 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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20	
... continues on next page ...	

...continued from previous page ...	
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 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: 2025-09-09T05:38:49Z	
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-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: 4.4) NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Windows	
Product detection result	
... continues on next page ...	

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
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 Version used: 2025-09-09T05:38:49Z
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-2022-21595 url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL advisory-id: cpuoct2022 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2022-1776 dfn-cert: DFN-CERT-2023-0504 dfn-cert: DFN-CERT-2022-2306

<p>Medium (CVSS: 4.3)</p> <p>NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Windows</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.5.20-log</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)</p>
<p>Summary</p> <p>Oracle MySQL Server is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.5.20</p> <p>Fixed version: 5.7.40</p> <p>Installation</p> <p>path / port: 3306/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 5.7.40, 8.0.17 or later.</p>
<p>Affected Software/OS</p> <p>Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.16.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Wi. ↵..</p> <p>OID:1.3.6.1.4.1.25623.1.0.118384</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2022-21589</p> <p>url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL</p> <p>advisory-id: cpuoct2022</p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2023-2031</p> <p>cert-bund: WID-SEC-2022-1776</p>
<p>... continues on next page ...</p>

...continued from previous page ...

dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.3)

NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 (Jul 2015)

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.

Quality of Detection (QoD): 80%**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.

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 (Jul 2015)

OID:1.3.6.1.4.1.25623.1.0.805930

Version used: 2025-09-09T05:38:49Z

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-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: 4.3) 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...	
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 Version used: 2025-09-09T05:38:49Z	
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-2022-21592 url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL advisory-id: cpuoct2022 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2022-1776 dfn-cert: DFN-CERT-2022-2306	

Medium (CVSS: 4.0) NVT: MySQL Unspecified vulnerability-06 (Jul 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.	
Quality of Detection (QoD): 80%	
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.	
... continues on next page ...	

...continued from previous page ...
Solution: Solution type: VendorFix Apply the patch from the referenced advisory.
Affected Software/OS 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 (Jul 2013) - Windows OID:1.3.6.1.4.1.25623.1.0.803728 Version used: 2025-09-09T05:38:49Z
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: MySQL Unspecified vulnerabilities-02 (Jul 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.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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 (Jul 2013) - Windows OID:1.3.6.1.4.1.25623.1.0.803724 Version used: 2025-09-09T05:38:49Z
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 dfn-cert: DFN-CERT-2013-1599 dfn-cert: DFN-CERT-2013-1553 dfn-cert: DFN-CERT-2013-1478

<p>Medium (CVSS: 4.0)</p> <p>NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - Windows</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.5.20-log</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↪25623.1.0.100152)</p>
<p>Summary</p> <p>Oracle MySQL Server is prone to an unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.5.20</p> <p>Fixed version: 5.5.23</p> <p>Installation</p> <p>path / port: 3306/tcp</p>
<p>Impact</p> <p>The flaw allows remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' package / privilege.</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 5.1.63, 5.5.23 or later.</p>
<p>Affected Software/OS</p> <p>Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - . ↪..</p> <p>OID:1.3.6.1.4.1.25623.1.0.117263</p> <p>Version used: 2025-09-09T05:38:49Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.5.20-log</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References</p> <p>cve: CVE-2012-1689</p>
<p>... continues on next page ...</p>

...continued from previous page ...
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMySQL
advisory-id: cpujul2012
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 <= 5.5.23 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.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
Product Detection Result ... continues on next page ...

...continued from previous page ...
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 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 <= 5.5.38 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.
Quality of Detection (QoD): 80%
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 ... continues on next page ...

...continued from previous page ...
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. Details: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804783 Version used: 2025-09-09T05:38:49Z
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-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 / 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 ... continues on next page ...

...continued from previous page ...
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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 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: 2025-09-09T05:38:49Z
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-2016-0596 url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMySQL 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: WID-SEC-2024-1482 cert-bund: CB-K16/1122
... continues on next page ...

...continued from previous page ...

```

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
dfn-cert: DFN-CERT-2016-0104

```

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.

Quality of Detection (QoD): 80%**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 availability via unknown vectors.

Solution:**Solution type:** VendorFix

Updates are available. Please see the references for more information.

... continues on next page ...

...continued from previous page ...
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: 2025-09-09T05:38:49Z
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-2016-0616 url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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: MySQL Unspecified vulnerabilities-01 (Jul 2013) - 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 MySQL is prone to multiple unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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 (Jul 2013) - Windows OID:1.3.6.1.4.1.25623.1.0.803723 Version used: 2025-09-09T05:38:49Z
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-2013-3804 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
... continues on next page ...

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20-log Fixed version: 5.5.22
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 OID:1.3.6.1.4.1.25623.1.0.803801 Version used: 2025-09-09T05:38:49Z
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-2012-1697 url: http://secunia.com/advisories/48890 url: http://www.securityfocus.com/bid/53064 url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#AppendixMySQL dfn-cert: DFN-CERT-2012-0939 dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 4.0) NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Jul 2014) - 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20-log Vulnerable range: 5.5 - 5.5.37
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 on Windows.
Vulnerability Insight Unspecified errors in the MySQL Server component via unknown vectors related to ENARC and SROPTZR.
... 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-03 (Jul 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804723 Version used: 2025-09-09T05:38:49Z
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-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_security_patches url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#AppendixMySQL 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 (Feb 2015) - 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.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page...	
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 (Feb 2015) - Windows OID:1.3.6.1.4.1.25623.1.0.805133 Version used: 2025-09-09T05:38:49Z	
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-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 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	

<p>Medium (CVSS: 4.0) NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability (Oct 2013) - Windows</p>
<p>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)</p>
<p>Summary Oracle MySQL is prone to an unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>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.</p>
<p>Solution: Solution type: VendorFix Apply the patch from the referenced advisory.</p>
<p>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.</p>
<p>Vulnerability Insight Unspecified error in the MySQL Server component via unknown vectors related to Optimizer.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability (Oct 2013) . ↵.. OID:1.3.6.1.4.1.25623.1.0.804033 Version used: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>References ... continues on next page ...</p>

...continued from previous page ...
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

Medium (CVSS: 4.0) NVT: Oracle MySQL Server Multiple Vulnerabilities - 03 - (Nov 2012) - 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.
Quality of Detection (QoD): 80%
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.
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 ... continues on next page ...

...continued from previous page ...
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 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803113 Version used: 2025-09-09T05:38:49Z
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-2012-3173 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: 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.5.31
... continues on next page ...

...continued from previous page...	
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	
	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: 2025-09-09T05:38:49Z
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.
...continues on next page...	

...continued from previous page ...
↔25623.1.0.100152)
Summary Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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.
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: 2025-09-09T05:38:49Z
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-2013-1512 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 (Feb 2015) - 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 unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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.
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 (Feb 2015) - Windows OID:1.3.6.1.4.1.25623.1.0.805135 Version used: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...

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-08 (Oct 2015) - 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.

Quality of Detection (QoD): 80%**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 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 (Oct 2015) - Windows

OID:1.3.6.1.4.1.25623.1.0.805771

Version used: 2025-09-09T05:38:49Z

... 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-2015-4816 url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html url: http://www.securityfocus.com/bid/77134 cert-bund: WID-SEC-2024-1483 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 dfn-cert: DFN-CERT-2015-1638
Medium (CVSS: 4.0) NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 (May 2014) - 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.
Quality of Detection (QoD): 80%
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 5.5.35 and earlier and 5.6.15 and earlier on Windows.
Vulnerability Insight 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 (May 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804574 Version used: 2025-09-09T05:38:49Z
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-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 - 03 (Jan 2014) - 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.
Quality of Detection (QoD): 80%
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 (Jan 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804074 Version used: 2025-09-09T05:38:49Z
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-2013-5891 url: http://secunia.com/advisories/56491 ... continues on next page ...

...continued from previous page ...
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 - 04 (Jan 2014) - 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.
Quality of Detection (QoD): 80%
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 5.1.72 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.
... 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 - 04 (Jan 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804075 Version used: 2025-09-09T05:38:49Z	
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-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 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 - 05 (Jan 2014) - 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 unspecified vulnerabilities.
Quality of Detection (QoD): 80%
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 (Jan 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804076 Version used: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...
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-02 (Jul 2015)
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.
Quality of Detection (QoD): 80%
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
... continues on next page ...

...continued from previous page ...
<p>Unspecified errors exist in the MySQL Server component via unknown vectors related to DML, Server : I_S, Server : Optimizer, and GIS.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Multiple Unspecified Vulnerabilities-02 (Jul 2015) OID:1.3.6.1.4.1.25623.1.0.805929 Version used: 2025-09-09T05:38:49Z</p>
<p>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)</p>
<p>References cve: CVE-2015-2648 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</p>
<p>Medium (CVSS: 4.0) NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 (Oct 2015) - Windows</p>
<p>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)</p>
<p>Summary Oracle MySQL is prone to multiple unspecified vulnerabilities.</p>
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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 (Oct 2015) - Windows OID:1.3.6.1.4.1.25623.1.0.805764 Version used: 2025-09-09T05:38:49Z
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-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
... continues on next page ...

...continued from previous page ...
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: WID-SEC-2024-1483
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: MySQL Unspecified vulnerability-04 (Jul 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.

Quality of Detection (QoD): 80%

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow remote 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.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: MySQL Unspecified vulnerability-04 (Jul 2013) - Windows OID:1.3.6.1.4.1.25623.1.0.803726 Version used: 2025-09-09T05:38:49Z
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

[[return to 192.168.1.207](#)]

2.1.21 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 based service enumeration reporting.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49152/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49152]

Port: 49153/tcp

UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49153]

Annotation: NRP server endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49153]

Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49153]

Annotation: DHCPv6 Client LRPC Endpoint

UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49153]

Annotation: Event log TCPIP

Port: 49154/tcp

UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

Annotation: IP Transition Configuration endpoint

UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

Annotation: XactSrv service

UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

Annotation: IKE/Authip API

UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49154]

Annotation: Impl friendly name

Port: 49155/tcp

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.1.207[49155]

... continues on next page ...

...continued from previous page...	
Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 49259/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.1.207[49259] Port: 49261/tcp UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.1.207[49261] Annotation: IPsec Policy agent endpoint Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.1.207[49261] Annotation: Remote Fw APIs Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting 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 information to gain more knowledge about the remote host and to conduct further attacks based on it.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.	
Affected Software/OS All systems exposing / disclosing information via DCE/RPC or MSRPC services.	
Vulnerability Insight 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 Method Reports previously collected (via 'DCE/RPC and MSRPC Services Enumeration' OID: 1.3.6.1.4.1.25623.1.0.108044) DCE/RPC or MSRPC services. This VT is reporting a severity by default. If the scanned network is e.g. a private LAN / private WAN which contains systems not accessible to the public (access restricted) and it is accepted that the service is disclosing information to this network please set the 'Network type' configuration of the following VT to e.g. 'Private LAN' or 'Private WAN': Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288) In this case a 'Log' level result is used instead. Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736	
... continues on next page ...	

...continued from previous page ...
Version used: 2025-11-26T05:40:08Z

[[return to 192.168.1.207](#)]

2.1.22 Medium 9200/tcp

Medium (CVSS: 6.5) NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)
Summary Elasticsearch is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 80%
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: 2025-09-03T08:26:15Z
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-2025-0933
... continues on next page ...

...continued from previous page...

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.

Quality of Detection (QoD): 80%**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 Vulnerability.
 ↪...

OID:1.3.6.1.4.1.25623.1.0.144431

Version used: 2025-09-03T08:26:15Z

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.
Quality of Detection (QoD): 80%
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: 2025-09-03T08:26:15Z
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/cert-bund: WID-SEC-2024-3184

Medium (CVSS: 5.3) NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)
... continues on next page ...

...continued from previous page ...	
Summary	Elasticsearch is prone to multiple vulnerabilities.
Quality of Detection (QoD):	80%
Vulnerability Detection Result	Installed version: 1.1.1 Fixed version: 6.8.15 Installation path / port: /
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: 2025-09-03T08:26:15Z
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 dfn-cert: DFN-CERT-2025-0933
Medium (CVSS: 4.9) NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)	
Summary	... continues on next page ...

...continued from previous page ...
Elasticsearch is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
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: 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: 2025-09-03T08:26:15Z
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 dfn-cert: DFN-CERT-2025-0933
Medium (CVSS: 4.3) NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows
Summary Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page ...
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 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: 2025-09-03T08:26:15Z
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 192.168.1.207](#)]

2.1.23 Medium 22/tcp

Medium (CVSS: 5.3) NVT: OpenSSH < 7.6 '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.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
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 Update to version 7.6 or later.
Affected Software/OS OpenSSH versions prior to 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 < 7.6 'sftp-server' Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.812050 Version used: 2024-12-13T05:05:32Z
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 url: http://www.securityfocus.com/bid/101552 url: https://github.com/openbsd/src/commit/a6981567e8e cert-bund: WID-SEC-2024-1082 cert-bund: CB-K20/0041 cert-bund: CB-K18/0137 cert-bund: CB-K17/2126 cert-bund: CB-K17/2014
... continues on next page ...

...continued from previous page ...
cert-bund: CB-K17/2002 dfn-cert: DFN-CERT-2024-1260 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 < 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 7.1 Fixed version: 7.8 Installation path / port: 22/tcp
Impact Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.
Solution: Solution type: VendorFix Update to version 7.8 or later.
Affected Software/OS OpenSSH versions 7.7 and prior.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>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</p>
<p>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: 2023-07-20T05:05:18Z</p>
<p>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)</p>
<p>References cve: CVE-2018-15473 url: https://0day.city/cve-2018-15473.html url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d↵1e0 cert-bund: WID-SEC-2024-1082 cert-bund: CB-K20/0041 cert-bund: CB-K18/1031 cert-bund: CB-K18/0873 dfn-cert: DFN-CERT-2024-1260 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</p>
Medium (CVSS: 5.3) NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows
<p>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)</p>
... continues on next page ...

...continued from previous page ...
Summary OpenSSH is prone to a user enumeration vulnerability.
Quality of Detection (QoD): 80%
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 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: WID-SEC-2024-1082
...continues on next page ...

...continued from previous page ...

```

cert-bund: CB-K18/0885
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2191

```

[\[return to 192.168.1.207 \]](#)**2.1.24 Medium 8181/tcp**

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

cpe:/a:ietf:transport_layer_security

Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
 ↪623.1.0.103692)

Summary

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

Quality of Detection (QoD): 99%**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.

... continues on next page ...

...continued from previous page ...
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: 2024-06-14T05:05:48Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)
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.
Quality of Detection (QoD): 70%
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.
... continues on next page ...

...continued from previous page ...
<p>Vulnerability Insight</p> <p>The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.</p> <p>Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:</p> <p>> 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.</p> <p>Both CVEs are still kept in this VT as a reference to the origin of this flaw.</p>
<p>Vulnerability Detection Method</p> <p>Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.</p> <p>Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)</p> <p>OID:1.3.6.1.4.1.25623.1.0.117761</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p>References</p> <p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</p> <p>cert-bund: WID-SEC-2026-0180</p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2024-0796</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K17/0980</p> <p>cert-bund: CB-K17/0979</p> <p>cert-bund: CB-K14/0772</p> <p>cert-bund: CB-K13/0915</p> <p>cert-bund: CB-K13/0462</p> <p>dfn-cert: DFN-CERT-2025-0933</p> <p>dfn-cert: DFN-CERT-2017-1013</p> <p>dfn-cert: DFN-CERT-2017-1012</p> <p>dfn-cert: DFN-CERT-2014-0809</p> <p>dfn-cert: DFN-CERT-2013-1928</p> <p>dfn-cert: DFN-CERT-2012-1112</p>
Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
<p>Product detection result</p> <p>cpe:/a:ietf:transport_layer_security</p>
...continues on next page ...

...continued from previous page ...
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)
Summary The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).
Quality of Detection (QoD): 99%
Vulnerability Detection Result The certificate of the remote service is signed by the following untrusted and/or dangerous CA: Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US 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
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: 2024-06-14T05:05:48Z
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: <code>cpe:/a:ietf:transport_layer_security</code> Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Product detection result <code>cpe:/a:ietf:transport_layer_security:1.1</code> Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - 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)
<p>Vulnerability Detection Method</p> <p>Checks the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2025-04-30T05:39:51Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:transport_layer_security:1.1</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p>References</p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>cve: CVE-2023-41928</p> <p>cve: CVE-2024-41270</p> <p>cve: CVE-2025-3200</p> <p>url: https://ssl-config.mozilla.org</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html</p> <p>url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch0eRichtlinien/TR03116/BSI-TR-03116-4.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html</p> <p>url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org</p> <p>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters0-report-2014</p> <p>url: https://datatracker.ietf.org/doc/rfc8996/</p> <p>url: https://vnhacker.blogspot.com/2011/09/beast.html</p> <p>url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</p> <p>url: https://certvde.com/en/advisories/VDE-2025-031/</p> <p>url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc</p> <p>url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273</p> <p>cert-bund: WID-SEC-2026-0180</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p>
...continues on next page ...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...

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
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

...continues on next page ...

...continued from previous page ...

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).

Quality of Detection (QoD): 80%

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

Affected Software/OS

All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.

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 Vulnerability.
↪..

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: 2025-03-27T05:38:50Z

References

url: <https://weakdh.org>

url: <https://weakdh.org/sysadmin.html>

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel>

... continues on next page ...

...continued from previous page ...
↪ines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/↪TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch↪eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes↪tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters↪-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile

[\[return to 192.168.1.207 \]](#)

2.1.25 Medium 8443/tcp

Medium (CVSS: 5.4) NVT: SSL/TLS: Report 'Anonymous' Cipher Suites
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
Summary This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DH_anon_WITH_AES_128_CBC_SHA
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
Solution: Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed 'Anonymous' cipher suites anymore. Please see the references for more resources supporting you in this task.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
All services providing an encrypted communication using 'Anonymous' SSL/TLS cipher suites.
Vulnerability Insight Services supporting 'Anonymous' cipher suites could allow a client to negotiate an SSL/TLS connection to the host without any authentication of the remote endpoint.
Vulnerability Detection Method Checks previous collected cipher suites. Details: SSL/TLS: Report 'Anonymous' Cipher Suites OID:1.3.6.1.4.1.25623.1.0.108147 Version used: 2025-03-27T05:38:50Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
References cve: CVE-2007-1858 cve: CVE-2014-0351 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch0eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters0-report-2014 url: https://web.archive.org/web/20210121181059/http://www.securityfocus.com/bid0/28482 url: https://web.archive.org/web/20210122052921/http://www.securityfocus.com/bid0/69754 cert-bund: CB-K14/0058 dfn-cert: DFN-CERT-2014-0049 dfn-cert: DFN-CERT-2012-0442
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Product detection result cpe:/a:ietf:transport_layer_security:1.0
... continues on next page ...

...continued from previous page ...
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can 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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
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 Checks 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: 2025-04-30T05:39:51Z
Product Detection Result
... continues on next page ...

...continued from previous page ...	
Product: cpe:/a:ietf:transport_layer_security:1.0	
Method: SSL/TLS: Version Detection	
OID: 1.3.6.1.4.1.25623.1.0.105782)	
References cve: CVE-2011-3389 cve: CVE-2015-0204 cve: CVE-2023-41928 cve: CVE-2024-41270 cve: CVE-2025-3200 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 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://certvde.com/en/advisories/VDE-2025-031/ url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273 cert-bund: WID-SEC-2026-0180 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	
... continues on next page ...	

...continued from previous page ...

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
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

...continues on next page ...

...continued from previous page ...

```

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
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).

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

... continues on next page ...

...continued from previous page...	
Server Temporary Key Size: 768 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. Please see the references for more resources supporting you with this task. - 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.	
Affected Software/OS All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.	
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 Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2025-03-27T05:38:50Z	
References url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↪-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile	

[[return to 192.168.1.207](#)]

2.1.26 Medium 8020/tcp

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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.1.207:8020/configurations.do:j_password
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
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: 2023-09-07T05:05:21Z
References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html

[\[return to 192.168.1.207 \]](#)

2.1.27 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 (cpu-jul2016) - 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.
Quality of Detection (QoD): 80%
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: 2025-09-09T05:38:49Z
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-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 (cpu-jul2016) - 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.
Quality of Detection (QoD): 80%
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.
... continues on next page ...

...continued from previous page ...
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 (. ↪.. OID:1.3.6.1.4.1.25623.1.0.808594 Version used: 2025-09-09T05:38:49Z
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-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 Unspecified Vulnerability-04 (Jul 2015)
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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: Apply the patch Installation path / port: 3306/tcp
... continues on next page ...

...continued from previous page ...
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 (Jul 2015) OID:1.3.6.1.4.1.25623.1.0.805931 Version used: 2025-09-09T05:38:49Z
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-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: 3.5) NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 (Oct 2015) - Windows
Product detection result
... continues on next page ...

...continued from previous page ...
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.
Quality of Detection (QoD): 80%
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.
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 (Oct 2015) - Windows OID:1.3.6.1.4.1.25623.1.0.805770 Version used: 2025-09-09T05:38:49Z
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-2015-4864 url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html url: http://www.securityfocus.com/bid/77187
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2024-1483
 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 Server Multiple Vulnerabilities - 05 - (Nov 2012) - 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.

Quality of Detection (QoD): 80%**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

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 - (Nov 2012) - Windows

OID:1.3.6.1.4.1.25623.1.0.803115

Version used: 2025-09-09T05:38:49Z

... 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-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: 2.8) NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 (Jan 2014) - 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.
Quality of Detection (QoD): 80%
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 (Jan 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804077 Version used: 2025-09-09T05:38:49Z	
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-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 <= 5.7.40, 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.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.7.41 Installation	
... continues on next page ...	

...continued from previous page ...	
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.	
↔...	
OID:1.3.6.1.4.1.25623.1.0.149532	
Version used: 2025-09-09T05:38:49Z	
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-2023-21963	
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL	
advisory-id: cpuapr2023	
cert-bund: WID-SEC-2024-1591	
cert-bund: WID-SEC-2023-1033	
dfn-cert: DFN-CERT-2023-0885	

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.	
Quality of Detection (QoD):	80%
Vulnerability Detection Result	
... continues on next page ...	

...continued from previous page ...	
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, 5.7.19 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: 2025-09-09T05:38:49Z	
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-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.	
... continues on next page ...	

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 5.5.20 Fixed version: 5.5.31 Installation 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: 2025-09-09T05:38:49Z
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 192.168.1.207](#)]

2.1.28 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.
Quality of Detection (QoD): 80%
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: 2025-09-03T08:26:15Z
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-2025-0933
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2022-1530

[\[return to 192.168.1.207 \]](#)**2.1.29 Low 22/tcp**

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):

umac-64-etm@openssh.com

umac-64@openssh.com

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
- 64-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: 2024-06-14T05:05:48Z

Referencesurl: <https://www.rfc-editor.org/rfc/rfc6668>url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>[\[return to 192.168.1.207 \]](#)

2.1.30 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.
Quality of Detection (QoD): 80%
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: 3883039921 Packet 2: 3883041007
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.
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: 2023-12-15T16:10:08Z
References url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 ... continues on next page ...

...continued from previous page ...

url: <https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

[\[return to 192.168.1.207 \]](#)

This file was automatically generated.