

# Scan Report

August 22, 2024

## Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.1.34”. The scan started at Thu Aug 22 08:04:31 2024 UTC and ended at Thu Aug 22 10:14:15 2024 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.1.34 . . . . .	2
2.1.1	High 4848/tcp . . . . .	3
2.1.2	High 8009/tcp . . . . .	5
2.1.3	High 22/tcp . . . . .	9
2.1.4	High 8282/tcp . . . . .	16
2.1.5	High 21/tcp . . . . .	38
2.1.6	High 1617/tcp . . . . .	39
2.1.7	High 9200/tcp . . . . .	40
2.1.8	High 8383/tcp . . . . .	43
2.1.9	High 80/tcp . . . . .	49
2.1.10	High 3306/tcp . . . . .	52
2.1.11	Medium 4848/tcp . . . . .	112
2.1.12	Medium 22/tcp . . . . .	123
2.1.13	Medium 8282/tcp . . . . .	128
2.1.14	Medium 21/tcp . . . . .	138
2.1.15	Medium 9200/tcp . . . . .	140
2.1.16	Medium 8383/tcp . . . . .	147
2.1.17	Medium 8181/tcp . . . . .	158
2.1.18	Medium 3306/tcp . . . . .	169

2.1.19	Medium 135/tcp . . . . .	285
2.1.20	Medium 3389/tcp . . . . .	287
2.1.21	Low 22/tcp . . . . .	294
2.1.22	Low general/tcp . . . . .	296
2.1.23	Low general/icmp . . . . .	297
2.1.24	Low 9200/tcp . . . . .	298
2.1.25	Low 3306/tcp . . . . .	299

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">192.168.1.34</a> <a href="#">vagrant-2008r2.home</a>	65	131	13	0	0
Total: 1	65	131	13	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 209 results selected by the filtering described above. Before filtering there were 479 results.

## 2 Results per Host

### 2.1 192.168.1.34

Host scan start Thu Aug 22 08:05:15 2024 UTC

Host scan end Thu Aug 22 10:14:04 2024 UTC

Service (Port)	Threat Level
<a href="#">4848/tcp</a>	High
<a href="#">8009/tcp</a>	High
<a href="#">22/tcp</a>	High
<a href="#">8282/tcp</a>	High
<a href="#">21/tcp</a>	High
<a href="#">1617/tcp</a>	High
<a href="#">9200/tcp</a>	High
<a href="#">8383/tcp</a>	High
<a href="#">80/tcp</a>	High
<a href="#">3306/tcp</a>	High
<a href="#">4848/tcp</a>	Medium
<a href="#">22/tcp</a>	Medium
<a href="#">8282/tcp</a>	Medium
<a href="#">21/tcp</a>	Medium
<a href="#">9200/tcp</a>	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
8383/tcp	Medium
8181/tcp	Medium
3306/tcp	Medium
135/tcp	Medium
3389/tcp	Medium
22/tcp	Low
general/tcp	Low
general/icmp	Low
9200/tcp	Low
3306/tcp	Low

### 2.1.1 High 4848/tcp

High (CVSS: 7.5)
NVT: Oracle Glass Fish Server Directory Traversal Vulnerability
<p><b>Summary</b> Glass fish server is prone to a directory traversal vulnerability.</p>
<p><b>Quality of Detection (QoD):</b> 99%</p>
<p><b>Vulnerability Detection Result</b> Vulnerable URL: https://vagrant-2008r2:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/windows/win.ini</p>
<p><b>Impact</b> Successful exploitation will allow remote attackers to gain access to sensitive information.</p>
<p><b>Solution:</b> <b>Solution type:</b> 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.</p>
<p><b>Affected Software/OS</b> Oracle Glassfish Server version 4.1.1 and probably prior.</p>
<p><b>Vulnerability Insight</b> The flaw is due to - Improper sanitization of parameter 'META-INF' in 'theme.php' file.</p>
<p>... continues on next page ...</p>

...continued from previous page ...
<b>Vulnerability Detection Method</b> Send a crafted request via HTTP GET and check whether it is able to get the content of passwd file. Details: Oracle Glass Fish Server Directory Traversal Vulnerability OID:1.3.6.1.4.1.25623.1.0.806848 Version used: 2023-07-20T05:05:17Z
<b>References</b> cve: CVE-2017-1000028 url: <a href="https://www.exploit-db.com/exploits/39241">https://www.exploit-db.com/exploits/39241</a>

High (CVSS: 7.5)
NVT: Oracle Glass Fish Server Directory Traversal Vulnerability
<b>Summary</b> Glass fish server is prone to a directory traversal vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerable URL: <a href="https://vagrant-2008r2.home:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/windows/win.ini">https://vagrant-2008r2.home:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/windows/win.ini</a>
<b>Impact</b> Successful exploitation will allow remote attackers to gain access to sensitive information.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Oracle Glassfish Server version 4.1.1 and probably prior.
<b>Vulnerability Insight</b> The flaw is due to - Improper sanitization of parameter 'META-INF' in 'theme.php' file.
<b>Vulnerability Detection Method</b> Send a crafted request via HTTP GET and check whether it is able to get the content of passwd file. Details: Oracle Glass Fish Server Directory Traversal Vulnerability
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.806848 Version used: 2023-07-20T05:05:17Z
<b>References</b> cve: CVE-2017-1000028 url: <a href="https://www.exploit-db.com/exploits/39241">https://www.exploit-db.com/exploits/39241</a>

[\[ return to 192.168.1.34 \]](#)

### 2.1.2 High 8009/tcp

High (CVSS: 9.8) NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)
<b>Summary</b> Apache Tomcat is prone to a remote code execution (RCE) vulnerability (dubbed 'Ghostcat') in the AJP connector.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> 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=92F1B61A8C0A9EC0206F4EA3 ↪4B707632; 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 <a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a> 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
...continues on next page ...

<p>...continued from previous page ...</p> <pre> http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd" version="3.1" metadata-complete="true"&gt; &lt;display-name&gt;Welcome to Tomcat&lt;/display-name&gt; &lt;description&gt;   Welcome to Tomcat &lt;/description&gt; &lt;/web-app&gt; AB \x0002\x0005\x0001 </pre>
<p><b>Solution:</b>  <b>Solution type:</b> VendorFix  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>
<p><b>Affected Software/OS</b>  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><b>Vulnerability Insight</b>  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><b>Vulnerability Detection Method</b>  Sends a crafted AJP request and checks the response.  Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat)  OID:1.3.6.1.4.1.25623.1.0.143545  Version used: 2024-06-28T15:38:46Z</p>
<p><b>References</b>  cve: CVE-2020-1938  cisa: Known Exploited Vulnerability (KEV) catalog  url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a>  url: <a href="https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1">https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1</a>  ↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E  url: <a href="https://www.chaitin.cn/en/ghostcat">https://www.chaitin.cn/en/ghostcat</a>  url: <a href="https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487">https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487</a>  url: <a href="https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi">https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi</a>  url: <a href="https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances">https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances</a>  ↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/  url: <a href="https://tomcat.apache.org/tomcat-7.0-doc/changelog.html">https://tomcat.apache.org/tomcat-7.0-doc/changelog.html</a>  url: <a href="https://tomcat.apache.org/tomcat-8.5-doc/changelog.html">https://tomcat.apache.org/tomcat-8.5-doc/changelog.html</a>  url: <a href="https://tomcat.apache.org/tomcat-9.0-doc/changelog.html">https://tomcat.apache.org/tomcat-9.0-doc/changelog.html</a>  cert-bund: WID-SEC-2024-0528  cert-bund: WID-SEC-2023-2480</p>
<p>... continues on next page ...</p>

...continued from previous page ...

```

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
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

```

High (CVSS: 9.8)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

**Summary**

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

**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=3E1715A5C91388594BEA196A
↳DE6B80AC; 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"
↳?>

```

&lt;!--

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,

...continues on next page ...



<p>...continued from previous page ...</p> <p>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.</p> <p>--&gt;</p> <pre>&lt;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"&gt;   &lt;display-name&gt;Welcome to Tomcat&lt;/display-name&gt;   &lt;description&gt;     Welcome to Tomcat   &lt;/description&gt; &lt;/web-app&gt; AB \x0002\x0005\x0001</pre>
<p><b>Solution:</b></p> <p><b>Solution type:</b> VendorFix</p> <p>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>
<p><b>Affected Software/OS</b></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><b>Vulnerability Insight</b></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><b>Vulnerability Detection Method</b></p> <p>Sends a crafted AJP request and checks the response. Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat) OID:1.3.6.1.4.1.25623.1.0.143545 Version used: 2024-06-28T15:38:46Z</p>
<p><b>References</b></p> <p>cve: CVE-2020-1938 cisa: Known Exploited Vulnerability (KEV) catalog url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> url: <a href="https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1?__hpid=hp%3Cannounce.tomcat.apache.org%3E">https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1?__hpid=hp%3Cannounce.tomcat.apache.org%3E</a> url: <a href="https://www.chaitin.cn/en/ghostcat">https://www.chaitin.cn/en/ghostcat</a> url: <a href="https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487">https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487</a> url: <a href="https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi">https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi</a></p>
<p>... continues on next page ...</p>

...continued from previous page ...
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances ↔-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
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
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

[\[ return to 192.168.1.34 \]](#)

### 2.1.3 High 22/tcp

High (CVSS: 9.8)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows
<b>Product detection result</b> cpe:/a:openbsd:openssh:7.1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>Summary</b> openssh is prone to a security bypass vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b>
... continues on next page ...

...continued from previous page ...
Installed version: 7.1 Fixed version: 7.2 Installation path / port: 22/tcp
<b>Impact</b> Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to OpenSSH version 7.2 or later.
<b>Affected Software/OS</b> OpenSSH versions before 7.2 on Windows
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810768 Version used: 2024-02-15T05:05:40Z
<b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b> cve: CVE-2016-1908 url: <a href="http://openwall.com/lists/oss-security/2016/01/15/13">http://openwall.com/lists/oss-security/2016/01/15/13</a> url: <a href="http://www.securityfocus.com/bid/84427">http://www.securityfocus.com/bid/84427</a> url: <a href="https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4">https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4</a> url: <a href="http://www.openssh.com/txt/release-7.2">http://www.openssh.com/txt/release-7.2</a> url: <a href="https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0↵db113c71e234416c">https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0↵db113c71e234416c</a> url: <a href="https://bugzilla.redhat.com/show_bug.cgi?id=1298741">https://bugzilla.redhat.com/show_bug.cgi?id=1298741</a> dfn-cert: DFN-CERT-2018-1828 dfn-cert: DFN-CERT-2016-1574 dfn-cert: DFN-CERT-2016-0754
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2016-0733  
 dfn-cert: DFN-CERT-2016-0488  
 dfn-cert: DFN-CERT-2016-0182

High (CVSS: 9.8)

NVT: SSH Brute Force Logins With Default Credentials Reporting

### Summary

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

Quality of Detection (QoD): 95%

### Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password>  
 vagrant:vagrant

### Impact

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

### Solution:

**Solution type:** Mitigation

Change the password as soon as possible.

### Affected Software/OS

The following products are known to use the default credentials checked by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) used for this reporting:

- CVE-2020-9473: S. Siedle & Soehne SG 150-0 Smart Gateway before 1.2.4
- CVE-2023-1944: minikube 1.29.0 and probably prior
- CVE-2024-22902: Vinchin Backup & Recovery
- CVE-2024-31970: AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1) during a window of time when the device is being set up
- Various additional products like e.g. Ubiquiti EdgeMax / EdgeRouter, Crestron AM-100 and similar for which no CVE was assigned (See 'default\_credentials.inc' file on the file system for a full list)

Other products might be affected as well.

### Vulnerability Insight

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

### Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013). Details: SSH Brute Force Logins With Default Credentials Reporting OID:1.3.6.1.4.1.25623.1.0.103239 Version used: 2024-07-26T05:05:35Z
<b>References</b> cve: CVE-1999-0501 cve: CVE-1999-0502 cve: CVE-1999-0507 cve: CVE-1999-0508 cve: CVE-2020-9473 cve: CVE-2023-1944 cve: CVE-2024-22902 cve: CVE-2024-31970

High (CVSS: 7.8)
NVT: OpenSSH Multiple Vulnerabilities (Jan 2017) - Windows
<b>Product detection result</b> cpe:/a:openbsd:openssh:7.1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>Summary</b> openssh is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 7.1 Fixed version: 7.4 Installation path / port: 22/tcp
<b>Impact</b> Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to OpenSSH version 7.4 or later.
... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> OpenSSH versions before 7.4 on Windows.
<b>Vulnerability Insight</b> Multiple flaws exist due to: <ul style="list-style-type: none"> <li>- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.</li> <li>- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.</li> <li>- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.</li> <li>- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.</li> <li>- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.</li> </ul>
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: OpenSSH Multiple Vulnerabilities (Jan 2017) - Windows OID:1.3.6.1.4.1.25623.1.0.810325 Version used: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b> cve: CVE-2016-10009 cve: CVE-2016-10010 cve: CVE-2016-10011 cve: CVE-2016-10012 cve: CVE-2016-10708 url: <a href="https://www.openssh.com/txt/release-7.4">https://www.openssh.com/txt/release-7.4</a> url: <a href="http://www.securityfocus.com/bid/94968">http://www.securityfocus.com/bid/94968</a> url: <a href="http://www.securityfocus.com/bid/94972">http://www.securityfocus.com/bid/94972</a> url: <a href="http://www.securityfocus.com/bid/94977">http://www.securityfocus.com/bid/94977</a> url: <a href="http://www.securityfocus.com/bid/94975">http://www.securityfocus.com/bid/94975</a> url: <a href="http://www.openwall.com/lists/oss-security/2016/12/19/2">http://www.openwall.com/lists/oss-security/2016/12/19/2</a> url: <a href="http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html">http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html</a> url: <a href="https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93c3e6b931de1d16737">https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93c3e6b931de1d16737</a> cert-bund: WID-SEC-2023-1996 cert-bund: CB-K18/0919 cert-bund: CB-K18/0591 cert-bund: CB-K18/0137 cert-bund: CB-K18/0041 dfn-cert: DFN-CERT-2021-0776 dfn-cert: DFN-CERT-2019-1408
...continues on next page ...

...continued from previous page ...

```

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 Denial of Service And User Enumeration Vulnerabilities - Windows

**Product detection result**

cpe:/a:openbsd:openssh:7.1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

**Summary**

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

**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.

... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to OpenSSH version 7.3 or later.
<b>Affected Software/OS</b> OpenSSH versions before 7.3 on Windows
<b>Vulnerability Insight</b> Multiple flaws exist due to: - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: OpenSSH Denial of Service And User Enumeration Vulnerabilities - Windows OID:1.3.6.1.4.1.25623.1.0.809121 Version used: 2024-02-15T05:05:40Z
<b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b> cve: CVE-2016-6515 cve: CVE-2016-6210 url: <a href="http://www.openssh.com/txt/release-7.3">http://www.openssh.com/txt/release-7.3</a> url: <a href="http://www.securityfocus.com/bid/92212">http://www.securityfocus.com/bid/92212</a> url: <a href="http://seclists.org/fulldisclosure/2016/Jul/51">http://seclists.org/fulldisclosure/2016/Jul/51</a> url: <a href="https://security-tracker.debian.org/tracker/CVE-2016-6210">https://security-tracker.debian.org/tracker/CVE-2016-6210</a> url: <a href="http://openwall.com/lists/oss-security/2016/08/01/2">http://openwall.com/lists/oss-security/2016/08/01/2</a> cert-bund: WID-SEC-2023-0450 cert-bund: WID-SEC-2023-0449 cert-bund: CB-K18/0041 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
...continues on next page ...



...continued from previous page ...

```
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
```

[\[ return to 192.168.1.34 \]](#)**2.1.4 High 8282/tcp****High (CVSS: 10.0)****NVT: Apache Axis2 Default Credentials (HTTP) - Active Check****Summary**

The remote Apache Axis2 web interface is using known default credentials.

**Quality of Detection (QoD): 98%****Vulnerability Detection Result**

It was possible to login at "http://vagrant-2008r2.home:8282/axis2/axis2-admin/"  
 ↪ using the following credentials (Username:Password):  
 - admin:axis2

**Impact**

This issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration or execute code by uploading malicious webservises.

**Solution:**

**Solution type:** Mitigation  
 Change the password.

**Vulnerability Insight**

It was possible to login with default credentials: admin/axis2

**Vulnerability Detection Method**

Tries to login with default credentials via HTTP.  
 Details: Apache Axis2 Default Credentials (HTTP) - Active Check  
 OID:1.3.6.1.4.1.25623.1.0.111006

... continues on next page ...

...continued from previous page ...
Version used: 2023-10-19T05:05:21Z
<b>References</b> cve: CVE-2010-0219 url: <a href="https://www.exploit-db.com/exploits/15869">https://www.exploit-db.com/exploits/15869</a> url: <a href="http://www.securityfocus.com/bid/44055">http://www.securityfocus.com/bid/44055</a> dfn-cert: DFN-CERT-2021-0775

High (CVSS: 10.0)
NVT: Apache Tomcat End of Life (EOL) Detection - Windows
<b>Product detection result</b> 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)
<b>Summary</b> The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> 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
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update the Apache Tomcat version on the remote host to a still supported version.
<b>Vulnerability Detection Method</b> Checks if an EOL version is present on the target host. Details: Apache Tomcat End of Life (EOL) Detection - Windows OID:1.3.6.1.4.1.25623.1.0.108134
... continues on next page ...

...continued from previous page ...
Version used: 2024-02-28T14:37:42Z
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> url: <a href="https://tomcat.apache.org/tomcat-10.0-eol.html">https://tomcat.apache.org/tomcat-10.0-eol.html</a> url: <a href="https://tomcat.apache.org/tomcat-85-eol.html">https://tomcat.apache.org/tomcat-85-eol.html</a> url: <a href="https://tomcat.apache.org/tomcat-80-eol.html">https://tomcat.apache.org/tomcat-80-eol.html</a> url: <a href="https://tomcat.apache.org/tomcat-70-eol.html">https://tomcat.apache.org/tomcat-70-eol.html</a> url: <a href="https://tomcat.apache.org/tomcat-60-eol.html">https://tomcat.apache.org/tomcat-60-eol.html</a> url: <a href="https://tomcat.apache.org/tomcat-55-eol.html">https://tomcat.apache.org/tomcat-55-eol.html</a> url: <a href="https://en.wikipedia.org/wiki/Apache_Tomcat#Releases">https://en.wikipedia.org/wiki/Apache_Tomcat#Releases</a> url: <a href="https://tomcat.apache.org/whichversion.html">https://tomcat.apache.org/whichversion.html</a>

High (CVSS: 10.0)
NVT: Apache Axis2 Default Credentials (HTTP) - Active Check
<b>Summary</b> The remote Apache Axis2 web interface is using known default credentials.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> It was possible to login at "http://vagrant-2008r2:8282/axis2/axis2-admin/" using the following credentials (Username:Password): - admin:axis2
<b>Impact</b> This issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration or execute code by uploading malicious webservicees.
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password.
<b>Vulnerability Insight</b> It was possible to login with default credentials: admin/axis2
<b>Vulnerability Detection Method</b> Tries to login with default credentials via HTTP.
... continues on next page ...

...continued from previous page ...
Details: Apache Axis2 Default Credentials (HTTP) - Active Check OID:1.3.6.1.4.1.25623.1.0.111006 Version used: 2023-10-19T05:05:21Z
<b>References</b> cve: CVE-2010-0219 url: <a href="https://www.exploit-db.com/exploits/15869">https://www.exploit-db.com/exploits/15869</a> url: <a href="http://www.securityfocus.com/bid/44055">http://www.securityfocus.com/bid/44055</a> dfn-cert: DFN-CERT-2021-0775

High (CVSS: 9.1)
NVT: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.42 Installation path / port: 8282/tcp
<b>Impact</b> Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.
<b>Affected Software/OS</b> 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...	
<b>Vulnerability Insight</b>	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.
<b>Vulnerability Detection Method</b>	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810764 Version used: 2024-02-15T05:05:40Z
<b>Product Detection Result</b>	Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b>	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 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
High (CVSS: 9.1)	
NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windows	
<b>Product detection result</b>	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)
<b>Summary</b>	... continues on next page ...

...continued from previous page ...	
Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.37 Installation path / port: 8282/tcp	
<b>Impact</b> Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Affected Software/OS</b> 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.	
<b>Vulnerability Insight</b> Multiple flaws exist due to: <ul style="list-style-type: none"> <li>- An error in the system property replacement feature for configuration files.</li> <li>- An error in the realm implementations in Apache Tomcat that does not process the supplied password if the supplied user name did not exist.</li> <li>- An error in the configured SecurityManager via a Tomcat utility method that is accessible to web applications.</li> <li>- An error in the configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.</li> <li>- 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.</li> </ul>	
<b>Vulnerability Detection Method</b> 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	
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation	
... continues on next page ...	

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> cve: CVE-2016-6794 cve: CVE-2016-0762 cve: CVE-2016-5018 cve: CVE-2016-6796 cve: CVE-2016-6797 url: <a href="http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72">http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72</a> url: <a href="http://www.securityfocus.com/bid/93940">http://www.securityfocus.com/bid/93940</a> url: <a href="http://www.securityfocus.com/bid/93944">http://www.securityfocus.com/bid/93944</a> url: <a href="http://www.securityfocus.com/bid/93939">http://www.securityfocus.com/bid/93939</a> url: <a href="http://www.securityfocus.com/bid/93942">http://www.securityfocus.com/bid/93942</a> url: <a href="http://www.securityfocus.com/bid/93943">http://www.securityfocus.com/bid/93943</a> url: <a href="http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47">http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47</a> url: <a href="http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10">http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8.5.6">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8.5.6</a> cert-bund: WID-SEC-2022-1910 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

High (CVSS: 7.5)

NVT: Apache Tomcat Security Bypass Vulnerability - Windows

#### Product detection result

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)

#### Summary

Apache Tomcat is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

#### Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
<b>Installed version:</b> 8.0.33 <b>Fixed version:</b> 8.0.44 <b>Installation path / port:</b> 8282/tcp
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.
<b>Affected Software/OS</b> 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
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> cve: CVE-2017-5664 url: <a href="https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b↪8b7896538478d760660%3Cannounce.tomcat.apache.org%3E">https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b↪8b7896538478d760660%3Cannounce.tomcat.apache.org%3E</a> url: <a href="http://www.securityfocus.com/bid/98888">http://www.securityfocus.com/bid/98888</a> cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0605
... continues on next page ...



...continued from previous page ...

```

cert-bund: CB-K18/0603
cert-bund: CB-K18/0478
cert-bund: CB-K18/0066
cert-bund: CB-K18/0047
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
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1011

```

High (CVSS: 7.5)

NVT: Apache Tomcat Reverse Proxy Information Disclosure 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 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

... continues on next page ...

...continued from previous page ...
Upgrade to version 9.0.0.M17, 8.5.11 or later.
<b>Affected Software/OS</b> 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.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810719 Version used: 2024-02-15T05:05:40Z
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> 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 dfn-cert: DFN-CERT-2017-0433
High (CVSS: 7.5)
NVT: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to an information disclosure vulnerability.
... continues on next page ...

...continued from previous page ...	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.43 Installation path / port: 8282/tcp	
<b>Impact</b> Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.	
<b>Affected Software/OS</b> 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.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windo. ↪... OID:1.3.6.1.4.1.25623.1.0.810762 Version used: 2024-02-15T05:05:40Z	
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
<b>References</b> cve: CVE-2017-5647 url: <a href="http://tomcat.apache.org/security-9.html">http://tomcat.apache.org/security-9.html</a> url: <a href="http://tomcat.apache.org/security-8.html">http://tomcat.apache.org/security-8.html</a> url: <a href="http://tomcat.apache.org/security-7.html">http://tomcat.apache.org/security-7.html</a> url: <a href="http://tomcat.apache.org/security-6.html">http://tomcat.apache.org/security-6.html</a> url: <a href="https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0↪dee9190ba48171451a0%3Cusers.tomcat.apache.org%3E">https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0↪dee9190ba48171451a0%3Cusers.tomcat.apache.org%3E</a>	
... continues on next page ...	

...continued from previous page ...
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0047
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
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.41 Installation path / port: 8282/tcp
<b>Impact</b> Successful exploitation will allow remote attackers to gain access to potentially sensitive information.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> ... continues on next page ...

...continued from previous page...	
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.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> 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	
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
<b>References</b> cve: CVE-2016-8745 url: <a href="https://bz.apache.org/bugzilla/show_bug.cgi?id=60409">https://bz.apache.org/bugzilla/show_bug.cgi?id=60409</a> url: <a href="http://www.securityfocus.com/bid/94828">http://www.securityfocus.com/bid/94828</a> url: <a href="http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15">http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41</a> url: <a href="http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75">http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9</a> url: <a href="http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50">http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50</a> cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2022-1375 cert-bund: CB-K18/0605 dfn-cert: DFN-CERT-2018-0729 dfn-cert: DFN-CERT-2017-1822 dfn-cert: DFN-CERT-2017-1095 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 'MultipartStream' Class DoS Vulnerability - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.36 Installation path / port: 8282/tcp
<b>Impact</b> Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.
<b>Affected Software/OS</b> 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.
<b>Vulnerability Insight</b> The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> cve: CVE-2016-3092 url: <a href="http://tomcat.apache.org/security-7.html">http://tomcat.apache.org/security-7.html</a> url: <a href="http://www.securityfocus.com/bid/91453">http://www.securityfocus.com/bid/91453</a> url: <a href="http://tomcat.apache.org/security-8.html">http://tomcat.apache.org/security-8.html</a> url: <a href="http://tomcat.apache.org/security-9.html">http://tomcat.apache.org/security-9.html</a> cert-bund: WID-SEC-2023-0644 cert-bund: WID-SEC-2022-1537 cert-bund: WID-SEC-2022-1375 cert-bund: CB-K18/0605 dfn-cert: DFN-CERT-2023-0574 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 '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)

**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

... continues on next page ...

...continued from previous page...	
Installation	
path / port:	8282/tcp
<b>Impact</b>	
Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.	
<b>Solution:</b>	
<b>Solution type:</b> 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.	
<b>Affected Software/OS</b>	
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.	
<b>Vulnerability Insight</b>	
The flaw exists due to a missing host name verification when using TLS with the WebSocket client.	
<b>Vulnerability Detection Method</b>	
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: 2024-02-15T05:05:40Z	
<b>Product Detection Result</b>	
Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
<b>References</b>	
cve: CVE-2018-8034 url: <a href="http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722091057.GA70283@minotaur.apache.org%3E">http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722091057.GA70283@minotaur.apache.org%3E</a> url: <a href="http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10">http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32</a> url: <a href="http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90">http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90</a> 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	
... continues on next page ...	



...continued from previous page ...

```

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 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**

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Vulnerability Detection Method</b>  Checks if a vulnerable version is present on the target host.  Details: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows  OID: 1.3.6.1.4.1.25623.1.0.104551  Version used: 2023-10-12T05:05:32Z</p>
<p><b>Product Detection Result</b>  Product: cpe:/a:apache:tomcat:8.0.33  Method: Apache Tomcat Detection Consolidation  OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p><b>References</b>  cve: CVE-2023-24998  url: <a href="https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1">https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1</a>  url: <a href="https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3">https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3</a>  url: <a href="https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5">https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5</a>  url: <a href="https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71">https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71</a>  url: <a href="https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85">https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85</a>  url: <a href="https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrdoy">https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrdoy</a>  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</p>
...continues on next page ...

...continued from previous page...

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  
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-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 'UTF-8 Decoder' Denial of Service Vulnerability - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.52 Installation path / port: 8282/tcp
<b>Impact</b> Successful exploitation will allow an attacker to conduct a denial-of-service condition.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> 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.
<b>Vulnerability Insight</b> The flaw exists due to improper handling of overflow in the UTF-8 decoder with supplementary characters.
<b>Vulnerability Detection Method</b> 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: 2024-02-15T05:05:40Z
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.107652)
<b>References</b> cve: CVE-2018-1336 url: <a href="http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090435.GA60759%40minotaur.apache.org%3E">http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090435.GA60759%40minotaur.apache.org%3E</a> url: <a href="http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8">http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31</a> url: <a href="http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52">http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52</a> 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: 7.1)

NVT: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows

**Product detection result**

cpe:/a:apache:tomcat:8.0.33

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)

**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

... continues on next page ...

...continued from previous page ...	
path / port:	8282/tcp
<b>Impact</b> 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.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.	
<b>Affected Software/OS</b> 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.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810717 Version used: 2024-02-15T05:05:40Z	
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
<b>References</b> cve: CVE-2016-6816 url: <a href="https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48">https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48</a> url: <a href="http://www.securityfocus.com/bid/94461">http://www.securityfocus.com/bid/94461</a> url: <a href="https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73">https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73</a> url: <a href="https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39">https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39</a> url: <a href="https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8">https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8</a> url: <a href="https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13">https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13</a> url: <a href="https://qualist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-information-disclosure">https://qualist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-information-disclosure</a> cert-bund: WID-SEC-2024-0528 dfn-cert: DFN-CERT-2017-1822 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-1068	
... continues on next page ...	

...continued from previous page ...
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

[\[ return to 192.168.1.34 \]](#)

### 2.1.5 High 21/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting
<b>Summary</b> It was possible to login into the remote FTP server using weak/known credentials.
<b>Quality of Detection (QoD):</b> 95%
<b>Vulnerability Detection Result</b> It was possible to login with the following credentials <User>:<Password> vagrant:vagrant
<b>Impact</b> This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
<b>Vulnerability Insight</b> The following devices are / software is known to be affected: - CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R - CVE-2013-7404: GE Healthcare Discovery NM 750b - CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices - CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
<b>Vulnerability Detection Method</b>
... continues on next page ...

...continued from previous page ...
<p>Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).</p> <p>Details: FTP Brute Force Logins Reporting</p> <p>OID:1.3.6.1.4.1.25623.1.0.108718</p> <p>Version used: 2023-12-06T05:06:11Z</p>
<p><b>References</b></p> <p>cve: CVE-1999-0501</p> <p>cve: CVE-1999-0502</p> <p>cve: CVE-1999-0507</p> <p>cve: CVE-1999-0508</p> <p>cve: CVE-2001-1594</p> <p>cve: CVE-2013-7404</p> <p>cve: CVE-2017-8218</p> <p>cve: CVE-2018-19063</p> <p>cve: CVE-2018-19064</p>

[\[ return to 192.168.1.34 \]](#)

### 2.1.6 High 1617/tcp

<p>High (CVSS: 7.5)</p> <p>NVT: Java JMX Insecure Configuration Vulnerability</p>
<p><b>Summary</b></p> <p>The Java JMX interface is configured in an insecure way by allowing unauthenticated attackers to load classes from any remote URL.</p>
<p><b>Quality of Detection (QoD): 70%</b></p>
<p><b>Vulnerability Detection Result</b></p> <p>It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the ↪ RMI port 49178/tcp without providing any credentials.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Enable password authentication and/or SSL client certificate authentication for the JMX agent.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Sends crafted RMI requests and checks the responses.</p> <p>Details: Java JMX Insecure Configuration Vulnerability</p> <p>OID:1.3.6.1.4.1.25623.1.0.143207</p> <p>Version used: 2020-11-10T09:46:51Z</p>
... continues on next page ...



...continued from previous page...

**References**

url: <https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/>  
 url: <https://www.optiv.com/blog/exploiting-jmx-rmi>  
 url: [https://www.rapid7.com/db/modules/exploit/multi/misc/java\\_jmx\\_server](https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server)

High (CVSS: 7.5)

NVT: Java JMX Insecure Configuration Vulnerability

**Summary**

The Java JMX interface is configured in an insecure way by allowing unauthenticated attackers to load classes from any remote URL.

Quality of Detection (QoD): 70%

**Vulnerability Detection Result**

It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the  
 ↪ RMI port 49178/tcp without providing any credentials.

**Solution:****Solution type:** Mitigation

Enable password authentication and/or SSL client certificate authentication for the JMX agent.

**Vulnerability Detection Method**

Sends crafted RMI requests and checks the responses.

Details: Java JMX Insecure Configuration Vulnerability

OID:1.3.6.1.4.1.25623.1.0.143207

Version used: 2020-11-10T09:46:51Z

**References**

url: <https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/>  
 url: <https://www.optiv.com/blog/exploiting-jmx-rmi>  
 url: [https://www.rapid7.com/db/modules/exploit/multi/misc/java\\_jmx\\_server](https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server)

[\[ return to 192.168.1.34 \]](#)

**2.1.7 High 9200/tcp**

High (CVSS: 10.0) NVT: Elasticsearch End of Life (EOL) Detection
<b>Summary</b> The Elasticsearch version on the remote host has reached the End of Life (EOL) and should not be used anymore.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> 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
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update Elasticsearch to a version that still receives technical support and updates.
<b>Vulnerability Detection Method</b> 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: 2023-07-20T05:05:17Z
<b>References</b> url: <a href="https://www.elastic.co/support/eol">https://www.elastic.co/support/eol</a>

High (CVSS: 9.8) NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows
<b>Summary</b> Elasticsearch is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 ... continues on next page ...

...continued from previous page ...	
<b>Fixed version:</b>	1.6.1
<b>Impact</b> Successful exploitation will allow remote attackers to execute code or read arbitrary files.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to Elasticsearch version 1.6.1, or later.	
<b>Affected Software/OS</b> Elasticsearch version 1.0.0 through 1.6.0 on Windows.	
<b>Vulnerability Insight</b> 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).	
<b>Vulnerability Detection Method</b> 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: 2024-02-15T05:05:40Z	
<b>References</b> cve: CVE-2015-5531 cve: CVE-2015-5377 url: <a href="https://www.elastic.co/community/security/">https://www.elastic.co/community/security/</a> url: <a href="http://www.securityfocus.com/bid/75935">http://www.securityfocus.com/bid/75935</a> url: <a href="http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded">http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded</a> cert-bund: CB-K15/1118 dfn-cert: DFN-CERT-2015-1160	

High (CVSS: 8.8)

NVT: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Windows

#### Summary

Elasticsearch is prone to an information disclosure vulnerability.

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

#### Vulnerability Detection Result

Installed version: 1.1.1

Fixed version: 5.6.12

...continues on next page ...

...continued from previous page ...	
<b>Impact</b>	Successful exploitation would allow an authenticated attacker to acquire valid login credentials.
<b>Solution:</b> <b>Solution type:</b> VendorFix	Update to version 5.6.12 or 6.4.1 respectively.
<b>Affected Software/OS</b>	Elasticsearch versions through 5.6.11 and 6.0.0 through 6.4.0.
<b>Vulnerability Insight</b>	The _cluster/settings API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.
<b>Vulnerability Detection Method</b>	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: 2024-02-15T05:05:40Z
<b>References</b>	cve: CVE-2018-3831 url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update ↔/149035 url: https://www.elastic.co/community/security dfn-cert: DFN-CERT-2020-1653

[\[ return to 192.168.1.34 \]](#)

2.1.8 High 8383/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
<b>Product detection result</b> 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)
<b>Summary</b>
... 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.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> '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)
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Services accepting vulnerable SSL/TLS cipher suites via HTTPS.
<b>Vulnerability Insight</b> 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).
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-2183 cve: CVE-2016-6329
... continues on next page ...

...continued from previous page ...

cve: CVE-2020-12872  
url: <https://bettercrypto.org/>  
url: <https://mozilla.github.io/server-side-tls/ssl-config-generator/>  
url: <https://sweet32.info/>  
cert-bund: WID-SEC-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  
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

...continues on next page ...

...continued from previous page ...

```

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

```

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><b>Solution:</b></p> <p><b>Solution type:</b> 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><b>Affected Software/OS</b></p> <p>Services accepting vulnerable SSL/TLS cipher suites via HTTPS.</p>
<p><b>Vulnerability Insight</b></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><b>Vulnerability Detection Method</b></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: 2024-06-14T05:05:48Z</p>
<p><b>Product Detection Result</b></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><b>References</b></p> <p>cve: CVE-2016-2183</p> <p>cve: CVE-2016-6329</p> <p>cve: CVE-2020-12872</p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a></p> <p>url: <a href="https://sweet32.info/">https://sweet32.info/</a></p> <p>cert-bund: WID-SEC-2024-1277</p> <p>cert-bund: WID-SEC-2024-0209</p> <p>cert-bund: WID-SEC-2024-0064</p> <p>cert-bund: WID-SEC-2022-2226</p> <p>cert-bund: WID-SEC-2022-1955</p> <p>cert-bund: CB-K21/1094</p> <p>cert-bund: CB-K20/1023</p> <p>cert-bund: CB-K20/0321</p> <p>cert-bund: CB-K20/0314</p> <p>cert-bund: CB-K20/0157</p>
... continues on next page ...



...continued from previous page ...

cert-bund: CB-K19/0618  
cert-bund: CB-K19/0615  
cert-bund: CB-K18/0296  
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  
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

...continues on next page ...

...continued from previous page ...
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

[\[ return to 192.168.1.34 \]](#)

### 2.1.9 High 80/tcp

High (CVSS: 10.0)
NVT: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check
<b>Product detection result</b> cpe:/a:microsoft:internet_information_services:7.5 Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: ↪ 1.3.6.1.4.1.25623.1.0.900710)
<b>Summary</b> This host is missing an important security update according to Microsoft Bulletin MS15-034.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
<b>Solution:</b> <b>Solution type:</b> VendorFix The vendor has released updates. Please see the references for more information.
<b>Affected Software/OS</b> - Microsoft Windows 8 x32/x64 - Microsoft Windows 8.1 x32/x64 - Microsoft Windows Server 2012 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior - Microsoft Windows 7 x32/x64 Service Pack 1 and prior
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Insight</b> Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.
<b>Vulnerability Detection Method</b> Sends a special crafted HTTP GET request and checks the response. Details: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check OID: 1.3.6.1.4.1.25623.1.0.105257 Version used: 2023-11-10T16:09:31Z
<b>Product Detection Result</b> Product: cpe:/a:microsoft:internet_information_services:7.5 Method: Microsoft Internet Information Services (IIS) Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900710
<b>References</b> cve: CVE-2015-1635 cisa: Known Exploited Vulnerability (KEV) catalog url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> url: <a href="https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy">https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy</a> ↪ s-could-allow-remote-code-execution-april-14-2015-e8755c1e-c5a8-fa75-c7b1-3208 ↪ 7b127850 url: <a href="https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m">https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m</a> ↪ s15-034 url: <a href="http://pastebin.com/ypURDPc4">http://pastebin.com/ypURDPc4</a> cert-bund: CB-K15/0527 dfn-cert: DFN-CERT-2015-0545
<b>High (CVSS: 10.0)</b> <b>NVT: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check</b>
<b>Product detection result</b> cpe:/a:microsoft:internet_information_services:7.5 Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: ↪ 1.3.6.1.4.1.25623.1.0.900710)
<b>Summary</b> This host is missing an important security update according to Microsoft Bulletin MS15-034.
<b>Quality of Detection (QoD): 70%</b>
<b>Vulnerability Detection Result</b> ... continues on next page ...

...continued from previous page ...
Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
<b>Solution:</b> <b>Solution type:</b> VendorFix The vendor has released updates. Please see the references for more information.
<b>Affected Software/OS</b> - Microsoft Windows 8 x32/x64 - Microsoft Windows 8.1 x32/x64 - Microsoft Windows Server 2012 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior - Microsoft Windows 7 x32/x64 Service Pack 1 and prior
<b>Vulnerability Insight</b> Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.
<b>Vulnerability Detection Method</b> Sends a special crafted HTTP GET request and checks the response. Details: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check OID:1.3.6.1.4.1.25623.1.0.105257 Version used: 2023-11-10T16:09:31Z
<b>Product Detection Result</b> Product: cpe:/a:microsoft:internet_information_services:7.5 Method: Microsoft Internet Information Services (IIS) Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900710)
<b>References</b> cve: CVE-2015-1635 cisa: Known Exploited Vulnerability (KEV) catalog url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> url: <a href="https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy">https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy</a> ↪s-could-allow-remote-code-execution-april-14-2015-e8755c1e-c5a8-fa75-c7b1-3208 ↪7b127850 url: <a href="https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m">https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m</a> ↪s15-034 url: <a href="http://pastebin.com/ypURDPc4">http://pastebin.com/ypURDPc4</a> cert-bund: CB-K15/0527 dfn-cert: DFN-CERT-2015-0545

[\[ return to 192.168.1.34 \]](#)

### 2.1.10 High 3306/tcp

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (cpuoct2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow a remote user to access restricted data.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.52 and prior, 5.6 through 5.6.33 and 5.7 through 5.7.15.
<b>Vulnerability Insight</b> Multiple flaws exist due to multiple unspecified errors in the 'Server: Security: Encryption' and 'Server: Logging' components.
<b>Vulnerability Detection Method</b> 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 ... continues on next page ...

...continued from previous page ...
Version used: 2021-10-13T11:01:26Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-5584 cve: CVE-2016-6662 cve: CVE-2016-7440 url: <a href="https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL</a> advisory-id: cpuoct2016 url: <a href="http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.txt">http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.txt</a> url: <a href="https://www.exploit-db.com/exploits/40360/">https://www.exploit-db.com/exploits/40360/</a> dfn-cert: DFN-CERT-2020-1473 dfn-cert: DFN-CERT-2017-0138 dfn-cert: DFN-CERT-2017-0060 dfn-cert: DFN-CERT-2016-1950 dfn-cert: DFN-CERT-2016-1859 dfn-cert: DFN-CERT-2016-1849 dfn-cert: DFN-CERT-2016-1790 dfn-cert: DFN-CERT-2016-1753 dfn-cert: DFN-CERT-2016-1714 dfn-cert: DFN-CERT-2016-1540 dfn-cert: DFN-CERT-2016-1479

High (CVSS: 9.8)

NVT: Oracle Mysql 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

...continues on next page ...

...continued from previous page ...	
Fixed version:	See reference
Installation path / port:	3306/tcp
<b>Impact</b> Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.	
<b>Solution:</b> <b>Solution type:</b> VendorFix The vendor has released updates. Please see the references for more information.	
<b>Affected Software/OS</b> 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.	
<b>Vulnerability Insight</b> Multiple flaws exist due to: <ul style="list-style-type: none"> <li>- An unspecified error within 'InnoDB (zlib)' component of MySQL Server.</li> <li>- An unspecified error within 'Server: Parser' component of MySQL Server.</li> <li>- An unspecified error within 'Client programs' component of MySQL Server.</li> <li>- An unspecified error within 'Server: Storage Engines' component of MySQL Server.</li> </ul>	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Update (cpuoct2018 - 02) - Windows OID:1.3.6.1.4.1.25623.1.0.814258 Version used: 2022-06-24T09:38:38Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2018-3133 cve: CVE-2018-3174 cve: CVE-2018-3282 cve: CVE-2016-9843 cve: CVE-2016-9840 cve: CVE-2016-9841 cve: CVE-2016-9842 url: <a href="https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL</a> advisory-id: cpuoct2018 cert-bund: WID-SEC-2024-1232	
... continues on next page ...	

...continued from previous page ...

```

cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/0714
cert-bund: CB-K18/1005
cert-bund: CB-K18/0799
cert-bund: CB-K18/0030
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

```

High (CVSS: 9.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

**Product detection result**

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

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.  
↪25623.1.0.100152)**Summary**

... continues on next page ...



...continued from previous page ...
It was possible to login into the remote MySQL as root using weak credentials.
<b>Quality of Detection (QoD): 95%</b>
<b>Vulnerability Detection Result</b> It was possible to login as root with an empty password.
<b>Solution:</b> <b>Solution type:</b> Mitigation - Change the password as soon as possible - Contact the vendor for other possible fixes / updates
<b>Affected Software/OS</b> The following products are known to use such weak credentials: - CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x - CVE-2004-2357: Proofpoint Protection Server - CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6 - CVE-2007-2554: Associated Press (AP) Newspaper 4.0.1 and earlier - CVE-2007-6081: AdventNet EventLog Analyzer build 4030 - CVE-2009-0919: XAMPP - CVE-2014-3419: Infoblox NetMRI before 6.8.5 - CVE-2015-4669: Xsuite 2.x - CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4 Other products might be affected as well.
<b>Vulnerability Detection Method</b> Details: MySQL / MariaDB Default Credentials (MySQL Protocol) OID:1.3.6.1.4.1.25623.1.0.103551 Version used: 2023-11-02T05:05:26Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2001-0645 cve: CVE-2004-2357 cve: CVE-2006-1451 cve: CVE-2007-2554 cve: CVE-2007-6081 cve: CVE-2009-0919 cve: CVE-2014-3419 cve: CVE-2015-4669 cve: CVE-2016-6531
... continues on next page ...

...continued from previous page ...

cve: CVE-2018-15719

High (CVSS: 9.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

**Product detection result**

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

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)

**Summary**

It was possible to login into the remote MySQL as root using weak credentials.

**Quality of Detection (QoD):** 95%**Vulnerability Detection Result**

It was possible to login as root with an empty password.

**Solution:****Solution type:** Mitigation

- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

**Affected Software/OS**

The following products are know to use such weak credentials:

- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030
- CVE-2009-0919: XAMPP
- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4

Other products might be affected as well.

**Vulnerability Detection Method**

Details: MySQL / MariaDB Default Credentials (MySQL Protocol)

OID:1.3.6.1.4.1.25623.1.0.103551

Version used: 2023-11-02T05:05:26Z

**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)
<b>References</b> cve: CVE-2001-0645 cve: CVE-2004-2357 cve: CVE-2006-1451 cve: CVE-2007-2554 cve: CVE-2007-6081 cve: CVE-2009-0919 cve: CVE-2014-3419 cve: CVE-2015-4669 cve: CVE-2016-6531 cve: CVE-2018-15719

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a vulnerability in libcurl.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.41 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.41, 8.0.32 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.40 and prior and 8.0 through 8.0.31.
<b>Vulnerability Detection Method</b> ... continues on next page ...

...continued from previous page...	
Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) ↔.. OID:1.3.6.1.4.1.25623.1.0.149170 Version used: 2023-10-13T05:06:10Z	- Win.
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2022-32221 cve: CVE-2022-35260 cve: CVE-2022-42915 cve: CVE-2022-42916 url: <a href="https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL</a> advisory-id: cpujan2023 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 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	
...continues on next page...	

...continued from previous page ...
dfn-cert: DFN-CERT-2022-2401
dfn-cert: DFN-CERT-2022-2400
dfn-cert: DFN-CERT-2022-2393
dfn-cert: DFN-CERT-2022-2391

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a vulnerability in InnoDB (zlib).
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.42 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.42, 8.0.32 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.31.
<b>Vulnerability Detection Method</b> 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: 2023-10-13T05:06:10Z
<b>Product Detection Result</b> 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-2022-37434

url: <https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL>

advisory-id: cpuapr2023

cert-bund: WID-SEC-2024-1653

cert-bund: WID-SEC-2024-1591

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

... continues on next page ...

...continued from previous page ...
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

<b>High (CVSS: 9.8)</b> <b>NVT: Oracle MySQL Server &lt;= 5.7.43, 8.x &lt;= 8.0.34, 8.1.0 Security Update (cpuoct2023) - Windows</b>
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.44 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.44, 8.0.35, 8.1.1 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.43 and prior, 8.x through 8.0.34 and 8.1.0.
<b>Vulnerability Detection Method</b> 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: 2023-10-27T16:11:33Z
<b>Product Detection Result</b> ... 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)
<b>References</b> cve: CVE-2023-38545 cve: CVE-2023-22084 cve: CVE-2023-38546 url: <a href="https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL</a> advisory-id: cpuoct2023 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-2024-1601 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
...continues on next page ...



...continued from previous page ...
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

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.39 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.39, 8.0.30 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.38 and prior and 8.0 through 8.0.29.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Wi. ↵.. OID:1.3.6.1.4.1.25623.1.0.148511 Version used: 2022-07-22T10:11:18Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2022-1292 cve: CVE-2022-27778 cve: CVE-2018-25032 cve: CVE-2022-21515 url: <a href="https://www.oracle.com/security-alerts/cpujul2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2022.html#AppendixMSQL</a> advisory-id: cpujul2022 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 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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K22/0570  
 cert-bund: CB-K22/0536  
 cert-bund: CB-K22/0386  
 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  
 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

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1049
dfn-cert: DFN-CERT-2022-0986
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.36 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.36, 8.0.27 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.35 and prior and 8.0 through 8.0.26.
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2021-10-23T08:58:44Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2021-3711 cve: CVE-2021-22926 cve: CVE-2021-35604 cve: CVE-2021-35624 cve: CVE-2021-22922 cve: CVE-2021-22923 cve: CVE-2021-22924 cve: CVE-2021-22925 cve: CVE-2021-22945 cve: CVE-2021-22946 cve: CVE-2021-22947 cve: CVE-2021-3712 url: <a href="https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL</a> advisory-id: cpuoct2021 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
...continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2022-0673
cert-bund:	WID-SEC-2022-0602
cert-bund:	WID-SEC-2022-0530
cert-bund:	WID-SEC-2022-0432
cert-bund:	WID-SEC-2022-0400
cert-bund:	WID-SEC-2022-0393
cert-bund:	WID-SEC-2022-0302
cert-bund:	WID-SEC-2022-0101
cert-bund:	WID-SEC-2022-0094
cert-bund:	CB-K22/0473
cert-bund:	CB-K22/0469
cert-bund:	CB-K22/0316
cert-bund:	CB-K22/0224
cert-bund:	CB-K22/0077
cert-bund:	CB-K22/0072
cert-bund:	CB-K22/0062
cert-bund:	CB-K22/0045
cert-bund:	CB-K22/0030
cert-bund:	CB-K22/0011
cert-bund:	CB-K21/1268
cert-bund:	CB-K21/1179
cert-bund:	CB-K21/1161
cert-bund:	CB-K21/1087
cert-bund:	CB-K21/0994
cert-bund:	CB-K21/0991
cert-bund:	CB-K21/0969
cert-bund:	CB-K21/0907
cert-bund:	CB-K21/0897
cert-bund:	CB-K21/0797
dfn-cert:	DFN-CERT-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
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2022-1215  
dfn-cert: DFN-CERT-2022-1143  
dfn-cert: DFN-CERT-2022-0933  
dfn-cert: DFN-CERT-2022-0922  
dfn-cert: DFN-CERT-2022-0867  
dfn-cert: DFN-CERT-2022-0835  
dfn-cert: DFN-CERT-2022-0666  
dfn-cert: DFN-CERT-2022-0586  
dfn-cert: DFN-CERT-2022-0437  
dfn-cert: DFN-CERT-2022-0369  
dfn-cert: DFN-CERT-2022-0122  
dfn-cert: DFN-CERT-2022-0120  
dfn-cert: DFN-CERT-2022-0118  
dfn-cert: DFN-CERT-2022-0112  
dfn-cert: DFN-CERT-2022-0076  
dfn-cert: DFN-CERT-2022-0052  
dfn-cert: DFN-CERT-2022-0031  
dfn-cert: DFN-CERT-2021-2527  
dfn-cert: DFN-CERT-2021-2502  
dfn-cert: DFN-CERT-2021-2481  
dfn-cert: DFN-CERT-2021-2438  
dfn-cert: DFN-CERT-2021-2434  
dfn-cert: DFN-CERT-2021-2403  
dfn-cert: DFN-CERT-2021-2394  
dfn-cert: DFN-CERT-2021-2369  
dfn-cert: DFN-CERT-2021-2329  
dfn-cert: DFN-CERT-2021-2223  
dfn-cert: DFN-CERT-2021-2216  
dfn-cert: DFN-CERT-2021-2214  
dfn-cert: DFN-CERT-2021-2189  
dfn-cert: DFN-CERT-2021-2188  
dfn-cert: DFN-CERT-2021-2185  
dfn-cert: DFN-CERT-2021-2167  
dfn-cert: DFN-CERT-2021-1996  
dfn-cert: DFN-CERT-2021-1931  
dfn-cert: DFN-CERT-2021-1917  
dfn-cert: DFN-CERT-2021-1915  
dfn-cert: DFN-CERT-2021-1871  
dfn-cert: DFN-CERT-2021-1803  
dfn-cert: DFN-CERT-2021-1799  
dfn-cert: DFN-CERT-2021-1743  
dfn-cert: DFN-CERT-2021-1593  
dfn-cert: DFN-CERT-2021-1580  
dfn-cert: DFN-CERT-2021-1568

High (CVSS: 9.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch
<b>Impact</b> Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced vendor advisory or upgrade to the latest version.
<b>Affected Software/OS</b> Oracle MySQL version 5.1.x to 5.1.64 and Oracle MySQL version 5.5.x to 5.5.26 on Windows.
<b>Vulnerability Insight</b> The flaws are due to multiple unspecified errors in MySQL server component related to server replication, information schema, protocol and server optimizer.
<b>Vulnerability Detection Method</b> Details: Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803111 Version used: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> ... continues on next page ...



...continued from previous page ...

```

cve: CVE-2012-3197
cve: CVE-2012-3163
cve: CVE-2012-3158
cve: CVE-2012-3150
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/55990
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56017
url: http://www.securityfocus.com/bid/56036
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118

```

**High (CVSS: 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%

**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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.49 and prior, 5.6 through 5.6.30 and 5.7 through 5.7.12.
<b>Vulnerability Insight</b> Multiple unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b> 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: 2023-11-03T05:05:46Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-3477 cve: CVE-2016-3521 cve: CVE-2016-3615 cve: CVE-2016-5440 url: <a href="https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/91902">http://www.securityfocus.com/bid/91902</a> url: <a href="http://www.securityfocus.com/bid/91932">http://www.securityfocus.com/bid/91932</a> url: <a href="http://www.securityfocus.com/bid/91960">http://www.securityfocus.com/bid/91960</a> url: <a href="http://www.securityfocus.com/bid/91953">http://www.securityfocus.com/bid/91953</a> advisory-id: cpujul2016 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: 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.

... continues on next page ...

...continued from previous page ...	
↔25623.1.0.100152)	
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.35 Installation path / port: 3306/tcp	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.35, 8.0.26 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.34 and prior and 8.0 through 8.0.25.	
<b>Vulnerability Detection Method</b> 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: 2023-10-20T16:09:12Z	
<b>Product Detection Result</b> 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)	
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL</a>	
... continues on next page ...	

...continued from previous page ...

advisory-id: cpujul2021  
 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-2022-1892  
 dfn-cert: DFN-CERT-2022-1692  
 dfn-cert: DFN-CERT-2022-1597  
 dfn-cert: DFN-CERT-2022-1241  
 dfn-cert: DFN-CERT-2022-0933  
 dfn-cert: DFN-CERT-2022-0872  
 dfn-cert: DFN-CERT-2022-0666  
 dfn-cert: DFN-CERT-2022-0076  
 dfn-cert: DFN-CERT-2022-0074  
 dfn-cert: DFN-CERT-2021-2527  
 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: 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)

...continues on next page ...

...continued from previous page ...
<b>Summary</b> Oracle MySQL is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the latest patch from vendor. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.59 and earlier, 5.6.39 and earlier, 5.7.21 and earlier on Windows
<b>Vulnerability Insight</b> Multiple flaws exist due to <ul style="list-style-type: none"> <li>- Multiple errors in the 'Client programs' component of MySQL Server.</li> <li>- An error in the 'Server: Locking' component of MySQL Server.</li> <li>- An error in the 'Server: Optimizer' component of MySQL Server.</li> <li>- Multiple errors in the 'Server: DDL' component of MySQL Server.</li> <li>- Multiple errors in the 'Server: Replication' component of MySQL Server.</li> <li>- An error in the 'InnoDB' component of MySQL Server.</li> <li>- An error in the 'Server : Security : Privileges' component of MySQL Server.</li> </ul>
<b>Vulnerability Detection Method</b> 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: 2024-02-29T14:37:57Z
<b>Product Detection Result</b> 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-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)

**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

... continues on next page ...

...continued from previous page ...
Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier, 5.7.17 and earlier on Windows
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2023-11-03T05:05:46Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2017-3309 cve: CVE-2017-3308 cve: CVE-2017-3329 cve: CVE-2017-3456 cve: CVE-2017-3453 cve: CVE-2017-3600 cve: CVE-2017-3462 cve: CVE-2017-3463 cve: CVE-2017-3461 cve: CVE-2017-3464 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html">http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html</a> url: <a href="http://www.securityfocus.com/bid/97742">http://www.securityfocus.com/bid/97742</a> url: <a href="http://www.securityfocus.com/bid/97725">http://www.securityfocus.com/bid/97725</a> url: <a href="http://www.securityfocus.com/bid/97763">http://www.securityfocus.com/bid/97763</a> url: <a href="http://www.securityfocus.com/bid/97831">http://www.securityfocus.com/bid/97831</a> url: <a href="http://www.securityfocus.com/bid/97776">http://www.securityfocus.com/bid/97776</a> url: <a href="http://www.securityfocus.com/bid/97765">http://www.securityfocus.com/bid/97765</a> url: <a href="http://www.securityfocus.com/bid/97851">http://www.securityfocus.com/bid/97851</a> url: <a href="http://www.securityfocus.com/bid/97849">http://www.securityfocus.com/bid/97849</a> url: <a href="http://www.securityfocus.com/bid/97812">http://www.securityfocus.com/bid/97812</a> url: <a href="http://www.securityfocus.com/bid/97818">http://www.securityfocus.com/bid/97818</a> cert-bund: CB-K18/0224 dfn-cert: DFN-CERT-2018-1276
... continues on next page ...

...continued from previous page ...
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 Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Windows	
<b>Product detection result</b> 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)	
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.42 Installation path / port: 3306/tcp	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.42, 8.0.33 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Win.↵.. OID:1.3.6.1.4.1.25623.1.0.149538 Version used: 2023-10-13T05:06:10Z	
... continues on next page ...	



...continued from previous page ...
<b>Product Detection Result</b> 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)
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL</a> advisory-id: cpuapr2023 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-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 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
...continues on next page ...

...continued from previous page ...	
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 <= 5.7.41, 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%

... continues on next page ...

...continued from previous page ...	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.42 Installation path / port: 3306/tcp	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.42, 8.0.31 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.30.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Win. ↔.. OID:1.3.6.1.4.1.25623.1.0.149534 Version used: 2023-10-13T05:06:10Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2023-21912 url: <a href="https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL</a> 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 <= 5.7.37 / 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)

... continues on next page ...

...continued from previous page ...
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.38 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.38, 8.0.29 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.37 and prior and 8.0 through 8.0.28.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Wi. ↪.. OID:1.3.6.1.4.1.25623.1.0.113944 Version used: 2022-04-25T14:30:15Z
<b>Product Detection Result</b> 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)
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixMSQL</a> advisory-id: cpuapr2022 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794
... continues on next page ...

...continued from previous page ...	
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
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-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
...continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603

High (CVSS: 7.5)

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

#### Product detection result

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

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)

#### Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

**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

... continues on next page ...

...continued from previous page...	
Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.147465 Version used: 2023-10-19T05:05:21Z	
<b>Product Detection Result</b> 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)	
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL</a> advisory-id: cpujan2022 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 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	
...continues on next page...	

...continued from previous page ...
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 Multiple Unspecified vulnerabilities-01 (Feb 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
<b>Impact</b> Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.5.40 and earlier, and 5.6.21 and earlier on Windows.
<b>Vulnerability Insight</b> 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...	
<b>Vulnerability Detection Method</b>	
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: 2024-02-09T05:06:25Z	
<b>Product Detection Result</b>	
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)	
<b>References</b>	
cve: CVE-2015-0411 cve: CVE-2014-6568 cve: CVE-2015-0382 cve: CVE-2015-0381 cve: CVE-2015-0374 url: <a href="http://secunia.com/advisories/62525">http://secunia.com/advisories/62525</a> url: <a href="http://www.securityfocus.com/bid/72191">http://www.securityfocus.com/bid/72191</a> url: <a href="http://www.securityfocus.com/bid/72210">http://www.securityfocus.com/bid/72210</a> url: <a href="http://www.securityfocus.com/bid/72200">http://www.securityfocus.com/bid/72200</a> url: <a href="http://www.securityfocus.com/bid/72214">http://www.securityfocus.com/bid/72214</a> url: <a href="http://www.securityfocus.com/bid/72227">http://www.securityfocus.com/bid/72227</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html">http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html</a> 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 <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Windows	
<b>Product detection result</b>	
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 ...	
<b>Summary</b>	Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b>	80%
<b>Vulnerability Detection Result</b>	Installed version: 5.5.20 Fixed version: 5.7.34 Installation path / port: 3306/tcp
<b>Solution:</b>	<b>Solution type:</b> VendorFix Update to version 5.7.34, 8.0.24 or later.
<b>Affected Software/OS</b>	Oracle MySQL Server version 5.7.33 and prior and 8.0 through 8.0.23.
<b>Vulnerability Detection Method</b>	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: 2023-10-20T16:09:12Z
<b>Product Detection Result</b>	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)
<b>References</b>	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
... continues on next page ...	

...continued from previous page ...

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-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  
cert-bund: WID-SEC-2022-0751  
cert-bund: WID-SEC-2022-0676  
cert-bund: WID-SEC-2022-0671  
cert-bund: WID-SEC-2022-0669  
cert-bund: WID-SEC-2022-0602  
cert-bund: CB-K22/0476  
cert-bund: CB-K22/0061  
cert-bund: CB-K21/1097  
cert-bund: CB-K21/1095  
cert-bund: CB-K21/1065  
cert-bund: CB-K21/0785  
cert-bund: CB-K21/0770  
cert-bund: CB-K21/0573  
cert-bund: CB-K21/0572  
cert-bund: CB-K21/0565  
cert-bund: CB-K21/0421  
cert-bund: CB-K21/0412  
cert-bund: CB-K21/0409  
cert-bund: CB-K21/0389  
cert-bund: CB-K21/0317  
cert-bund: CB-K21/0185  
dfn-cert: DFN-CERT-2022-1582  
dfn-cert: DFN-CERT-2022-1571  
dfn-cert: DFN-CERT-2022-1241  
dfn-cert: DFN-CERT-2022-1215  
dfn-cert: DFN-CERT-2022-0933  
dfn-cert: DFN-CERT-2022-0666  
dfn-cert: DFN-CERT-2022-0121  
dfn-cert: DFN-CERT-2022-0076  
dfn-cert: DFN-CERT-2022-0024  
dfn-cert: DFN-CERT-2021-2527  
dfn-cert: DFN-CERT-2021-2394  
dfn-cert: DFN-CERT-2021-2223  
dfn-cert: DFN-CERT-2021-2216  
dfn-cert: DFN-CERT-2021-2214  
dfn-cert: DFN-CERT-2021-2197  
dfn-cert: DFN-CERT-2021-2196

...continues on next page ...

...continued from previous page ...

```

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
dfn-cert: DFN-CERT-2021-1549
dfn-cert: DFN-CERT-2021-1547
dfn-cert: DFN-CERT-2021-1537
dfn-cert: DFN-CERT-2021-1500
dfn-cert: DFN-CERT-2021-1418
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1132
dfn-cert: DFN-CERT-2021-1129
dfn-cert: DFN-CERT-2021-1128
dfn-cert: DFN-CERT-2021-1098
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0984
dfn-cert: DFN-CERT-2021-0884
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0829
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0818
dfn-cert: DFN-CERT-2021-0813
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0696
dfn-cert: DFN-CERT-2021-0656
dfn-cert: DFN-CERT-2021-0630
dfn-cert: DFN-CERT-2021-0629
dfn-cert: DFN-CERT-2021-0409
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2021-0363

```

High (CVSS: 7.5)

NVT: Oracle MySQL Server &lt;= 5.6.48 Security Update (cpujul2020) - 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.49 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.49 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.48 and prior.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows OID:1.3.6.1.4.1.25623.1.0.144286 Version used: 2021-08-16T12:00:57Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2020-1967 cve: CVE-2020-14539 cve: CVE-2020-14559 url: <a href="https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL</a> advisory-id: cpujul2020 cert-bund: WID-SEC-2024-0794 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
... continues on next page ...

...continued from previous page ...

```

cert-bund: CB-K20/0711
cert-bund: CB-K20/0708
cert-bund: CB-K20/0357
dfn-cert: DFN-CERT-2021-2192
dfn-cert: DFN-CERT-2021-0830
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0140
dfn-cert: DFN-CERT-2020-2295
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1788
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-0956
dfn-cert: DFN-CERT-2020-0930
dfn-cert: DFN-CERT-2020-0841
dfn-cert: DFN-CERT-2020-0824
dfn-cert: DFN-CERT-2020-0822

```

High (CVSS: 7.5)

NVT: Oracle MySQL 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)**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:**

... continues on next page ...

...continued from previous page ...	
<b>Solution type:</b> VendorFix Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.	
<b>Affected Software/OS</b> Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Windows	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2017-3302 url: <a href="https://bugs.mysql.com/bug.php?id=63363">https://bugs.mysql.com/bug.php?id=63363</a> url: <a href="https://bugs.mysql.com/bug.php?id=70429">https://bugs.mysql.com/bug.php?id=70429</a> url: <a href="http://www.openwall.com/lists/oss-security/2017/02/11/11">http://www.openwall.com/lists/oss-security/2017/02/11/11</a> cert-bund: CB-K18/0224 dfn-cert: DFN-CERT-2018-1276 dfn-cert: DFN-CERT-2018-0242 dfn-cert: DFN-CERT-2017-1675 dfn-cert: DFN-CERT-2017-1341 dfn-cert: DFN-CERT-2017-1282 dfn-cert: DFN-CERT-2017-0675 dfn-cert: DFN-CERT-2017-0430	

High (CVSS: 7.5)

NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpuoct2023) - 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.43 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.43, 8.0.34 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.
<b>Vulnerability Detection Method</b> 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: 2023-10-20T05:06:03Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2023-2650 cve: CVE-2023-0464 cve: CVE-2023-0465 cve: CVE-2023-0466 cve: CVE-2023-1255 url: <a href="https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL</a> advisory-id: cpuoct2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0120
... continues on next page ...



...continued from previous page ...

cert-bund: WID-SEC-2024-0064  
cert-bund: WID-SEC-2024-0053  
cert-bund: WID-SEC-2023-2917  
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-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

<b>High (CVSS: 7.5)</b> <b>NVT: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows</b>
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation path / port:         3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to cause the affected application to crash, resulting in a denial-of-service condition.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.54 and earlier, 5.6.20 and earlier on Windows
<b>Vulnerability Insight</b> The flaw exists due to some unspecified error in the 'Server: C API' component due to failure to handle exceptional conditions.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows OID:1.3.6.1.4.1.25623.1.0.810880 Version used: 2023-07-14T16:09:27Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2017-3302 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html">http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html</a> url: <a href="http://www.securityfocus.com/bid/96162">http://www.securityfocus.com/bid/96162</a> cert-bund: CB-K18/0224 dfn-cert: DFN-CERT-2018-1276 dfn-cert: DFN-CERT-2018-0242 dfn-cert: DFN-CERT-2017-1675 dfn-cert: DFN-CERT-2017-1341 dfn-cert: DFN-CERT-2017-1282 dfn-cert: DFN-CERT-2017-0675 dfn-cert: DFN-CERT-2017-0430

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
... continues on next page ...

...continued from previous page ...	
<b>Affected Software/OS</b>	Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.
<b>Vulnerability Insight</b>	An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Option' sub-component.
<b>Vulnerability Detection Method</b>	Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.808591 Version used: 2022-07-07T10:16:06Z
<b>Product Detection Result</b>	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)
<b>References</b>	cve: CVE-2016-3471 url: <a href="https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/91913">http://www.securityfocus.com/bid/91913</a> advisory-id: cpujul2016 dfn-cert: DFN-CERT-2016-1192 dfn-cert: DFN-CERT-2016-1169

High (CVSS: 7.5)	
NVT: Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Windows	
<b>Product detection result</b>	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)
<b>Summary</b>	Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b>	80%
<b>Vulnerability Detection Result</b>	Installed version: 5.5.20 Fixed version: 5.5.40
... continues on next page ...	

...continued from previous page ...	
<b>Installation</b>	
path / port:	3306/tcp
<b>Impact</b>	
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.	
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
Update to version 5.5.40, 5.6.21 or later.	
<b>Affected Software/OS</b>	
Oracle MySQL Server versions 5.5.39 and prior and 5.6 through 5.6.20.	
<b>Vulnerability Insight</b>	
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.	
<b>Vulnerability Detection Method</b>	
Checks if a vulnerable version is present on the target host.	
Details: Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Wi.	
↔..	
OID:1.3.6.1.4.1.25623.1.0.804781	
Version used: 2022-04-14T11:24:11Z	
<b>Product Detection Result</b>	
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)	
<b>References</b>	
cve: CVE-2014-6507	
cve: CVE-2014-6491	
cve: CVE-2014-6500	
cve: CVE-2014-6469	
cve: CVE-2014-6555	
cve: CVE-2014-6559	
cve: CVE-2014-6494	
cve: CVE-2014-6496	
cve: CVE-2014-6464	
url: <a href="https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL</a>	
url: <a href="http://www.securityfocus.com/bid/70444">http://www.securityfocus.com/bid/70444</a>	
url: <a href="http://www.securityfocus.com/bid/70446">http://www.securityfocus.com/bid/70446</a>	
... continues on next page ...	

...continued from previous page ...

```

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: 7.2)

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**

... continues on next page ...

...continued from previous page ...
Successful exploitation will allow an remote attacker to gain elevated privileges on the affected system, also could allow buffer overflow attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to Oracle MySQL Server 5.5.52 or later.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.x to 5.5.51 on windows
<b>Vulnerability Insight</b> Multiple errors exist. Please see the references for more information.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> url: <a href="http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html">http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html</a>

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a vulnerability in the parser.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
... continues on next page ...

...continued from previous page ...	
Fixed version:	5.7.30
Installation path / port:	3306/tcp
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
Update to version 5.7.30, 8.0.20 or later.	
<b>Affected Software/OS</b>	
Oracle MySQL Server version 5.7.29 and prior and 8.0 through 8.0.19.	
<b>Vulnerability Detection Method</b>	
Checks if a vulnerable version is present on the target host.	
Details: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Wi.	
↔..	
OID:1.3.6.1.4.1.25623.1.0.145800	
Version used: 2021-08-26T13:01:12Z	
<b>Product Detection Result</b>	
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)	
<b>References</b>	
cve: CVE-2021-2144	
url: <a href="https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL</a>	
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 Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan2016) - Windows	
<b>Product detection result</b>	
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)	
<b>Summary</b>	
...continues on next page ...	



...continued from previous page ...
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.46 and prior, 5.6 through 5.6.27 and version 5.7.9.
<b>Vulnerability Insight</b> Unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan20. ↔.. OID:1.3.6.1.4.1.25623.1.0.806876 Version used: 2022-04-13T13:17:10Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-0608 cve: CVE-2016-0609 cve: CVE-2016-0606 cve: CVE-2016-0600 cve: CVE-2016-0598 cve: CVE-2016-0597 cve: CVE-2016-0546 cve: CVE-2016-0505
... continues on next page ...

...continued from previous page ...
url: <a href="https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMySQL">https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMySQL</a>
url: <a href="http://www.securityfocus.com/bid/81258">http://www.securityfocus.com/bid/81258</a>
url: <a href="http://www.securityfocus.com/bid/81226">http://www.securityfocus.com/bid/81226</a>
url: <a href="http://www.securityfocus.com/bid/81188">http://www.securityfocus.com/bid/81188</a>
url: <a href="http://www.securityfocus.com/bid/81182">http://www.securityfocus.com/bid/81182</a>
url: <a href="http://www.securityfocus.com/bid/81151">http://www.securityfocus.com/bid/81151</a>
url: <a href="http://www.securityfocus.com/bid/81066">http://www.securityfocus.com/bid/81066</a>
url: <a href="http://www.securityfocus.com/bid/81088">http://www.securityfocus.com/bid/81088</a>
advisory-id: cpujan2016
cert-bund: WID-SEC-2024-1482
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

#### 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:

... continues on next page ...

...continued from previous page ...
<b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server Server 5.5.44 and earlier, and 5.6.25 and earlier
<b>Vulnerability Insight</b> Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-4879 cve: CVE-2015-4819 url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html">http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html</a> url: <a href="http://www.securityfocus.com/bid/77140">http://www.securityfocus.com/bid/77140</a> url: <a href="http://www.securityfocus.com/bid/77196">http://www.securityfocus.com/bid/77196</a> cert-bund: WID-SEC-2024-1483 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
<b>Product detection result</b>
... 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service attack and partially modify data.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.19 and earlier on Windows
<b>Vulnerability Insight</b> The flaw exists due to an error in 'Server:Partition' component.
<b>Vulnerability Detection Method</b> 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: 2024-02-29T14:37:57Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2018-2562 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html">http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html</a> cert-bund: CB-K18/0480
...continues on next page ...

...continued from previous page ...

```

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 &lt;= 5.6.42 / 5.7 &lt;= 5.7.24 / 8.0 &lt;= 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)

**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**

... continues on next page ...

...continued from previous page ...
Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2023-02-02T10:09:00Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2019-2534 cve: CVE-2019-2529 cve: CVE-2019-2482 cve: CVE-2019-2455 cve: CVE-2019-2503 cve: CVE-2018-0734 cve: CVE-2019-2537 cve: CVE-2019-2481 cve: CVE-2019-2507 cve: CVE-2019-2531 cve: CVE-2018-5407 url: <a href="https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL</a> advisory-id: cpujan2019 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
... continues on next page ...

...continued from previous page ...

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  
 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

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2018-2396 dfn-cert: DFN-CERT-2018-2360 dfn-cert: DFN-CERT-2018-2338 dfn-cert: DFN-CERT-2018-2214
<b>High (CVSS: 7.0)</b> NVT: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (cpuoct2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation of these vulnerabilities will allow remote authenticated attackers to cause denial of service conditions and gain elevated privileges.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.51 and prior, 5.6 through 5.6.32 and 5.7 through 5.7.14.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 (
... continues on next page ...



...continued from previous page ...
↩️.. OID:1.3.6.1.4.1.25623.1.0.809372 Version used: 2021-10-13T11:01:26Z
<b>Product Detection Result</b> 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)
<b>References</b> 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 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

[\[ return to 192.168.1.34 \]](#)

### 2.1.11 Medium 4848/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired
<b>Product detection result</b> 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)
...continues on next page ...

...continued from previous page...	
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.	
<b>Quality of Detection (QoD): 99%</b>	
<b>Vulnerability Detection Result</b> 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	
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.	
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> 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)						
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.						
<b>Quality of Detection (QoD):</b> 70%						
<b>Vulnerability Detection Result</b> 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 ----- ↪----- <table><tr><td>TLSv1.0</td><td>  10</td></tr><tr><td>TLSv1.1</td><td>  10</td></tr><tr><td>TLSv1.2</td><td>  10</td></tr></table>	TLSv1.0	10	TLSv1.1	10	TLSv1.2	10
TLSv1.0	10					
TLSv1.1	10					
TLSv1.2	10					
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.						
<b>Solution:</b> <b>Solution type:</b> 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.						
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.						
<b>Vulnerability Insight</b> 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.						
<b>Vulnerability Detection Method</b> 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 ... continues on next page ...						

...continued from previous page ...
Version used: 2024-07-24T05:06:37Z
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego ↪tiation-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-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
<b>Product detection result</b> 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)
<b>Summary</b> The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> The certificate of the remote service is signed by the following untrusted and/o ↪r dangerous CA: Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ ↪ia,C=US Certificate details: fingerprint (SHA-1)   4A5758F59279E82F2A913C83CA658D6964575A72 fingerprint (SHA-256)   AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD ... continues on next page ...

...continued from previous page ...	
↔5B23381002A885F556	
issued by	CN=localhost,OU=GlassFish,O=Oracle Corporation
↔,L=Santa Clara,ST=California,C=US	
public key algorithm	RSA
public key size (bits)	2048
serial	04A9972F
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost,OU=GlassFish,O=Oracle Corporation
↔,L=Santa Clara,ST=California,C=US	
subject alternative names (SAN)	None
valid from	2013-05-15 05:33:38 UTC
valid until	2023-05-13 05:33:38 UTC
<b>Impact</b> An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.	
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate with one signed by a trusted CA.	
<b>Vulnerability Detection Method</b> 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	
<b>Product Detection Result</b> 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)	
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	
<b>Quality of Detection (QoD):</b> 70%	
<b>Vulnerability Detection Result</b> The following indicates that the remote SSL/TLS service is affected: Protocol Version   Successful re-done SSL/TLS handshakes (Renegotiation) over an	
... continues on next page ...	

...continued from previous page...	
↔ existing / already established SSL/TLS connection	
-----	
↔-----	
TLSv1.0	10
TLSv1.1	10
TLSv1.2	10
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> 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: 2024-07-24T05:06:37Z	
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> 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-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b>
... continues on next page ...

...continued from previous page ...
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 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
... continues on next page ...



...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868

...continues on next page ...

...continued from previous page ...

```

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 &lt; 2048).

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

... continues on next page ...

...continued from previous page ...
<b>Server Temporary Key Size: 1024 bits</b>
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2023-07-21T05:05:22Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> ... continues on next page ...

...continued from previous page ...
<b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2023-07-21T05:05:22Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

[\[ return to 192.168.1.34 \]](#)

### 2.1.12 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows
<b>Product detection result</b> cpe:/a:openbsd:openssh:7.1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>Summary</b> OpenSSH is prone to a user enumeration vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 7.1 Fixed version: None
... continues on next page ...

...continued from previous page...	
<b>Installation</b>	
path / port:	22/tcp
<b>Impact</b>	Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.
<b>Solution:</b>	
<b>Solution type:</b>	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.
<b>Affected Software/OS</b>	OpenSSH version 5.9 through 7.8.
<b>Vulnerability Insight</b>	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.
<b>Vulnerability Detection Method</b>	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
<b>Product Detection Result</b>	Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b>	cve: CVE-2018-15919 url: <a href="https://bugzilla.novell.com/show_bug.cgi?id=1106163">https://bugzilla.novell.com/show_bug.cgi?id=1106163</a> url: <a href="https://seclists.org/oss-sec/2018/q3/180">https://seclists.org/oss-sec/2018/q3/180</a> cert-bund: WID-SEC-2024-1082 cert-bund: CB-K18/0885 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2018-2293 dfn-cert: DFN-CERT-2018-2191

Medium (CVSS: 5.3)
NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows
<b>Product detection result</b> cpe:/a:openbsd:openssh:7.1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>Summary</b> OpenSSH is prone to a user enumeration vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 7.1 Fixed version: 7.8 Installation path / port: 22/tcp
<b>Impact</b> Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 7.8 or later.
<b>Affected Software/OS</b> OpenSSH versions 7.7 and prior.
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b> cve: CVE-2018-15473 url: <a href="https://0day.city/cve-2018-15473.html">https://0day.city/cve-2018-15473.html</a> url: <a href="https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d">https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d</a> ↪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

Medium (CVSS: 5.3)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability - Windows
<b>Product detection result</b> cpe:/a:openbsd:openssh:7.1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>Summary</b> openssh is prone to a security bypass vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 7.1 Fixed version: 7.6 Installation path / port: 22/tcp
<b>Impact</b> ... continues on next page ...

...continued from previous page...
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to OpenSSH version 7.6 or later.
<b>Affected Software/OS</b> OpenSSH versions before 7.6 on Windows
<b>Vulnerability Insight</b> The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: OpenSSH 'sftp-server' Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.812050 Version used: 2024-02-15T05:05:40Z
<b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:7.1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
<b>References</b> cve: CVE-2017-15906 url: <a href="https://www.openssh.com/txt/release-7.6">https://www.openssh.com/txt/release-7.6</a> url: <a href="http://www.securityfocus.com/bid/101552">http://www.securityfocus.com/bid/101552</a> url: <a href="https://github.com/openbsd/src/commit/a6981567e8e">https://github.com/openbsd/src/commit/a6981567e8e</a> cert-bund: WID-SEC-2024-1082 cert-bund: CB-K20/0041 cert-bund: CB-K18/0137 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

[\[ return to 192.168.1.34 \]](#)



**2.1.13 Medium 8282/tcp**

Medium (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files
<b>Product detection result</b> 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)
<b>Summary</b> The Apache Tomcat servlet/JSP container has default files installed.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> The following default files were found : http://vagrant-2008r2:8282/examples/servlets/index.html http://vagrant-2008r2:8282/examples/jsp/snp/snoop.jsp http://vagrant-2008r2:8282/examples/jsp/index.html
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.
<b>Vulnerability Insight</b> Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)

Medium (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files
<b>Product detection result</b> 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)
<b>Summary</b> The Apache Tomcat servlet/JSP container has default files installed.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> The following default files were found : http://vagrant-2008r2.home:8282/examples/servlets/index.html http://vagrant-2008r2.home:8282/examples/jsp/snp/snoop.jsp http://vagrant-2008r2.home:8282/examples/jsp/index.html
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.
<b>Vulnerability Insight</b> Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:apache:tomcat:8.0.33 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)

Medium (CVSS: 6.5)
NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Apache Tomcat is prone to multiple access bypass vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 8.0.33 Fixed version: 8.0.50 Installation path / port: 8282/tcp
<b>Impact</b> Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.
<b>Affected Software/OS</b> 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.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit.
... continues on next page ...

...continued from previous page ...

↔..

OID:1.3.6.1.4.1.25623.1.0.812784

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

**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-2018-1305

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

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 Axis2 <= 1.6.2 Multiple Vulnerabilities
<b>Summary</b> Apache Axis2 is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.6.0 Fixed version: None Installation path / port: /axis2
<b>Impact</b> Successfully exploiting these issues allows attackers to: <ul style="list-style-type: none"> <li>- CVE-2012-5785: perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks</li> <li>- 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</li> <li>- CVE-2012-5351: allows remote attackers to forge messages and bypass authentication</li> </ul>
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> The issue affects versions up to 1.6.2.
<b>Vulnerability Insight</b> The following flaws exist: <ul style="list-style-type: none"> <li>- CVE-2012-5785: a security-bypass vulnerability because the application fails to properly validate SSL certificates from the server</li> <li>- CVE-2012-4418: a security vulnerability involving XML signature wrapping</li> <li>- CVE-2012-5351: a SAML assertion that lacks a Signature element, aka a 'Signature exclusion attack'</li> </ul>
<b>Vulnerability Detection Method</b> 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: 2023-12-20T05:05:58Z
... continues on next page ...

...continued from previous page ...

**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>  
 url: <http://www.securityfocus.com/bid/55508>

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://vagrant-2008r2.home:8282/host-manager/html:Tomcat Host Manager Application>  
<http://vagrant-2008r2.home:8282/manager/html:Tomcat Manager Application>  
<http://vagrant-2008r2.home: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

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)

... continues on next page ...

...continued from previous page ...
<p>- HTTP Forms (e.g. Login) with input field of type 'password'</p> <p>Details: Cleartext Transmission of Sensitive Information via HTTP</p> <p>OID:1.3.6.1.4.1.25623.1.0.108440</p> <p>Version used: 2023-09-07T05:05:21Z</p>
<p><b>References</b></p> <p>url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a></p> <p>url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a></p> <p>url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a></p>

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
<p><b>Summary</b></p> <p>The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p>
<b>Quality of Detection (QoD):</b> 80%
<p><b>Vulnerability Detection Result</b></p> <p>The following URLs requires Basic Authentication (URL:realm name):</p> <p><a href="http://vagrant-2008r2:8282/host-manager/html">http://vagrant-2008r2:8282/host-manager/html</a>:"Tomcat Host Manager Application"</p> <p><a href="http://vagrant-2008r2:8282/manager/html">http://vagrant-2008r2:8282/manager/html</a>:"Tomcat Manager Application"</p> <p><a href="http://vagrant-2008r2:8282/manager/status">http://vagrant-2008r2:8282/manager/status</a>:"Tomcat Manager Application"</p>
<p><b>Impact</b></p> <p>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.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Workaround</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
... continues on next page ...

...continued from previous page ...
<p>The script is currently checking the following:</p> <ul style="list-style-type: none"> <li>- HTTP Basic Authentication (Basic Auth)</li> <li>- HTTP Forms (e.g. Login) with input field of type 'password'</li> </ul> <p>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</p>
<p><b>References</b></p> <p>url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a></p> <p>url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a></p> <p>url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a></p>

Medium (CVSS: 4.3)
NVT: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows
<p><b>Product detection result</b></p> <p>cpe:/a:apache:tomcat:8.0.33</p> <p>Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)</p>
<p><b>Summary</b></p> <p>Apache Tomcat is prone to an information disclosure vulnerability.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>Installed version: 8.0.33</p> <p>Fixed version: 8.5.86</p> <p>Installation</p> <p>path / port: 8282/tcp</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> VendorFix</p> <p>Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.</p>
<p><b>Affected Software/OS</b></p> <p>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.</p>
<p><b>Vulnerability Insight</b></p> <p>... continues on next page ...</p>



...continued from previous page...

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](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](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](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](https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86)

cert-bund: WID-SEC-2024-1238

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-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

Medium (CVSS: 4.3)
NVT: Apache Tomcat Open Redirect Vulnerability - Windows
<p><b>Product detection result</b></p> <p>cpe:/a:apache:tomcat:8.0.33</p> <p>Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)</p>
<p><b>Summary</b></p> <p>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.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>Installed version: 8.0.33</p> <p>Fixed version: 8.5.34</p> <p>Installation path / port: 8282/tcp</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> VendorFix</p> <p>Update to version 7.0.91, 8.5.34, 9.0.12 or later.</p>
<p><b>Affected Software/OS</b></p> <p>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.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache Tomcat Open Redirect Vulnerability - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.141569</p> <p>Version used: 2024-02-15T05:05:40Z</p>
<p><b>Product Detection Result</b></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><b>References</b></p> <p>cve: CVE-2018-11784</p> <p>url: <a href="http://tomcat.apache.org/security-9.html">http://tomcat.apache.org/security-9.html</a></p> <p>url: <a href="http://tomcat.apache.org/security-8.html">http://tomcat.apache.org/security-8.html</a></p> <p>... continues on next page ...</p>

...continued from previous page ...
url: http://tomcat.apache.org/security-7.html
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

[\[ return to 192.168.1.34 \]](#)

2.1.14 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Quality of Detection (QoD): 70%</b>
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Non-anonymous sessions: 331 Password required for openvasvt. Anonymous sessions: 331 Password required for anonymous.
<b>Impact</b>
... continues on next page ...

...continued from previous page ...
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: 2023-12-20T05:05:58Z

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Non-anonymous sessions: 331 Password required for openvasvt. Anonymous sessions: 331 Password required for anonymous.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: 2023-12-20T05:05:58Z

[\[ return to 192.168.1.34 \]](#)

2.1.15 Medium 9200/tcp

Medium (CVSS: 6.8)
NVT: Elastisearch RCE Vulnerability
<b>Summary</b> Elasticsearch is prone to a remote code execution (RCE) vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerable URL: http://vagrant-2008r2.home:9200/_search?source=%7B%22size%22%3A1%2C%22query%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%22script_fields%22%3A%7B%22VTest%22%3A%7B%22script%22%3A%22import%20java.util.*%3B%5Cimport%20java.io.*%3B%5Cnew%20Scanner(new%20File(%5C%22%2Fwindows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D%7D%7D&callback=?
<b>Impact</b> An attacker can exploit this issue to execute arbitrary code
<b>Solution:</b> <b>Solution type:</b> VendorFix Ask the vendor for an update or disable 'dynamic scripting'
<b>Affected Software/OS</b> Elasticsearch < 1.2
<b>Vulnerability Insight</b> Elasticsearch has a flaw in its default configuration which makes it possible for any webpage to execute arbitrary code on visitors with Elasticsearch installed.
<b>Vulnerability Detection Method</b> Send a special crafted HTTP GET request and check the response Details: Elastisearch RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.105032 Version used: 2024-06-28T05:05:33Z
... continues on next page ...

... continued from previous page ...

## References

cve: CVE-2014-3120

cisa: Known Exploited Vulnerability (KEV) catalog

url: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

```
url: http://bouk.co/blog/elasticsearch-rce/
```

cert-bund: CB-K14/1131

dfn-cert: DFN-CERT-2014-1188

## Summary

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

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

## Vulnerability Detection Result

Vulnerable URL: [http://vagrant-2008r2:9200/\\_search?source=%2B%22size%22%3A1%2C%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match\\_all%22%3A%7B%7D%7D%22script\\_fields%22%3A%7B%22VTest%22%3A%7B%22script%22%3A%22import%20java.util.\\*%3B%5Cnimport%20java.io.\\*%3B%5Cnnew%20Scanner\(new%20File\(%5C%22%2Fwindows%2Fwin.ini%5C%22\)\).useDelimiter\(%5C%22%5C%5C%5C%5CZ%5C%22\).next\(\)%3B%22%7D%7D%7D&callback=?](http://vagrant-2008r2:9200/_search?source=%2B%22size%22%3A1%2C%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%22script_fields%22%3A%7B%22VTest%22%3A%7B%22script%22%3A%22import%20java.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2Fwindows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D%7D%7D&callback=?)

## Impact

An attacker can exploit this issue to execute arbitrary code

**Solution:**

**Solution type:** VendorFix

Ask the vendor for an update or disable 'dynamic scripting'

**Affected Software/OS**

Elasticsearch &lt; 1.2

## Vulnerability Insight

Elasticsearch has a flaw in its default configuration which makes it possible for any webpage to execute arbitrary code on visitors with Elasticsearch installed.

## Vulnerability Detection Method

Send a special crafted HTTP GET request and check the response

## Details: Elasticsearch RCE Vulnerability

OID:1.3.6.1.4.1.25623.1.0.105032

Version used: 2024-06-28T05:05:33Z

...continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2014-3120  
 cisa: Known Exploited Vulnerability (KEV) catalog  
 url: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>  
 url: <http://bouk.co/blog/elasticsearch-rce/>  
 cert-bund: CB-K14/1131  
 dfn-cert: DFN-CERT-2014-1188

Medium (CVSS: 6.5)

NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

**Summary**

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

**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: 2021-08-17T12:00:57Z

**References**

cve: CVE-2021-22144  
 url: <https://discuss.elastic.co/t/elasticsearch-7-13-3-and-6-8-17-security-updat↵e/278100>

... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2022-1777
dfn-cert: DFN-CERT-2022-2315

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability - Windows
<b>Summary</b> Elasticsearch is prone to a field disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 6.8.12 Installation path / port: /
<b>Impact</b> An attacker could gain additional permissions against a restricted index.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.8.12, 7.9.1 or later.
<b>Affected Software/OS</b> Elasticsearch prior to version 6.8.12 and 7.9.0.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerabilit. ↪.. OID:1.3.6.1.4.1.25623.1.0.144431 Version used: 2024-02-15T05:05:40Z
<b>References</b> cve: CVE-2020-7019 url: <a href="https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update/245456">https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update/245456</a> ↪/245456



Medium (CVSS: 5.9)  NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) - Windows
<b>Summary</b> Elasticsearch is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 6.8.2 Installation path / port: /
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.8.2 or 7.2.1 respectively.
<b>Affected Software/OS</b> Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.
<b>Vulnerability Insight</b> A race condition flaw was found in the response headers Elasticsearch returns to a request.
<b>Vulnerability Detection Method</b> 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: 2024-02-19T05:05:57Z
<b>References</b> cve: CVE-2019-7614 url: <a href="https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/192963">https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/192963</a> ↪ url: <a href="https://www.elastic.co/community/security/">https://www.elastic.co/community/security/</a>

Medium (CVSS: 5.3)
NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)
<b>Summary</b> Elasticsearch is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 6.8.15 Installation path / port: /
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.8.15, 7.12.0 or later.
<b>Affected Software/OS</b> Elasticsearch versions prior to versions 6.8.15 or 7.12.0.
<b>Vulnerability Insight</b> The following vulnerabilities exist: - CVE-2021-22135: Suggester & Profile API information disclosure flaw - CVE-2021-22137: Field disclosure flaw
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08) OID:1.3.6.1.4.1.25623.1.0.145940 Version used: 2021-08-17T12:00:57Z
<b>References</b> cve: CVE-2021-22135 cve: CVE-2021-22137 url: <a href="https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updates/268125">https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updates/268125</a> cert-bund: WID-SEC-2022-0720

Medium (CVSS: 4.9)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)
<b>Summary</b> Elasticsearch is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 6.8.14 Installation path / port: /
<b>Impact</b> This could allow an Elasticsearch administrator to view sensitive details.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.8.14, 7.10.0 or later.
<b>Affected Software/OS</b> Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03) OID:1.3.6.1.4.1.25623.1.0.145383 Version used: 2021-08-17T12:00:57Z
<b>References</b> cve: CVE-2020-7021 url: <a href="https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-update/263915">https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-update/263915</a> url: <a href="https://www.elastic.co/community/security">https://www.elastic.co/community/security</a>

Medium (CVSS: 4.3)
NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows
<b>Summary</b> Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 1.4.0.Beta1
<b>Impact</b> Successful exploitation will allow remote attackers to inject arbitrary web script or HTML.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to Elasticsearch version 1.4.0.Beta1, or later.
<b>Affected Software/OS</b> Elasticsearch version 1.3.x and prior on Windows.
<b>Vulnerability Insight</b> The Flaw is due to an error in the CORS functionality.
<b>Vulnerability Detection Method</b> 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: 2024-02-15T05:05:40Z
<b>References</b> cve: CVE-2014-6439 url: <a href="https://www.elastic.co/community/security/">https://www.elastic.co/community/security/</a> url: <a href="http://www.securityfocus.com/bid/70233">http://www.securityfocus.com/bid/70233</a> url: <a href="http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded">http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded</a>

[\[ return to 192.168.1.34 \]](#)

### 2.1.16 Medium 8383/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
<b>Summary</b> 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.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> 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)
<b>Impact</b> Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.
<b>Vulnerability Insight</b> SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf">https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</a>

Medium (CVSS: 5.0)
NVT: '/WEB-INF/' Information Disclosure Vulnerability (HTTP)
<b>Summary</b> Various application or web servers / products are prone to an information disclosure vulnerability.
... continues on next page ...

...continued from previous page ...

**Quality of Detection (QoD): 99%****Vulnerability Detection Result**

Vulnerable URL: https://vagrant-2008r2.home:8383/WEB-INF./web.xml

Response (truncated):

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
<!-- Added for MickeyClient Pdf Generation -->
<context-param>
  <param-name>ContextPath</param-name>
  <param-value>/</param-value>
</context-param>
<context-param>
  <param-name>defaultSkin</param-name>
  <param-value>woody</param-value>
</context-param>
<context-param>
  <param-name>useInstantFeedback</param-name>
  <param-value>true</param-value>
</context-param>
<context-param>
  <param-name>mailServerName</param-name>
  <param-value>smtp.india.adventnet.com</param-value>
</context-param>
<context-param>
  <param-name>instantFeedbackAddress</param-name>
  <param-value>sym-issues@adventnet.com</param-value>
</context-param>
<context-param>
  <param-name>AUTO_IMPORT_USER</param-name>
  <param-value>false</param-value>
</context-param>
<context-param>
  <param-name>PARAMETER-ENCODING</param-name>
  <param-value>UTF-8</param-value>
</context-param>
<listener>
  <listener-class>com.adventnet.sym.webclient.configurations.SymHttpSessionBindi
ngListener</listener-class>
</listener>
<!-- SDP-DC integration -->
  <listener>

```

...continues on next page ...

...continued from previous page ...
<pre> &lt;listener-class&gt;com.adventnet.sym.webclient.common.DCSessionListener&lt;/listener ↵-class&gt; &lt;/listener&gt; &lt;!-- SDP-DC integra </pre>
<p><b>Impact</b></p> <p>Based on the information provided in this file an attacker might be able to gather additional info and / or sensitive data about the application / the application / web server.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> VendorFix</p> <p>Please contact the vendor for more information on possible fixes.</p>
<p><b>Affected Software/OS</b></p> <p>The following products are known to be affected:</p> <ul style="list-style-type: none"> <li>- A misconfigured reverse proxy.</li> </ul> <p>Other products might be affected as well.</p>
<p><b>Vulnerability Insight</b></p> <p>The servlet specification prohibits servlet containers from serving resources in the '/WEB-INF' and '/META-INF' directories of a web application archive directly to clients.</p> <p>This means that URLs like:</p> <p><a href="http://example.com/WEB-INF/web.xml">http://example.com/WEB-INF/web.xml</a></p> <p>will return an error message, rather than the contents of the deployment descriptor.</p> <p>However, some application or web servers / products are prone to a vulnerability that exposes this information if the client requests a URL like this instead:</p> <p><a href="http://example.com/META-INF./web.xml">http://example.com/META-INF./web.xml</a></p> <p>(note the 'f.' in 'WEB-INF').</p>
<p><b>Vulnerability Detection Method</b></p> <p>Sends a crafted HTTP GET request and checks the response.</p> <p>Details: '/WEB-INF./' Information Disclosure Vulnerability (HTTP)</p> <p>OID:1.3.6.1.4.1.25623.1.0.117225</p> <p>Version used: 2023-03-06T10:19:58Z</p>
<p><b>References</b></p> <p>url: <a href="https://bz.apache.org/bugzilla/show_bug.cgi?id=60667">https://bz.apache.org/bugzilla/show_bug.cgi?id=60667</a></p>

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

... continues on next page ...

...continued from previous page ...	
↪623.1.0.103692)	
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.	
<b>Quality of Detection (QoD): 99%</b>	
<b>Vulnerability Detection Result</b> The certificate of the remote service expired on 2020-09-05 12:24:44. Certificate details: fingerprint (SHA-1)   701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315 fingerprint (SHA-256)   C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E ↪B135AD83CD7B01A5A5 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	
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.	
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> 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
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274
... continues on next page ...

...continued from previous page ...
Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 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
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2016-1164  
dfn-cert: DFN-CERT-2016-0388  
dfn-cert: DFN-CERT-2015-1853  
dfn-cert: DFN-CERT-2015-1332  
dfn-cert: DFN-CERT-2015-0884  
dfn-cert: DFN-CERT-2015-0800  
dfn-cert: DFN-CERT-2015-0758  
dfn-cert: DFN-CERT-2015-0567  
dfn-cert: DFN-CERT-2015-0544  
dfn-cert: DFN-CERT-2015-0530  
dfn-cert: DFN-CERT-2015-0396  
dfn-cert: DFN-CERT-2015-0375  
dfn-cert: DFN-CERT-2015-0374  
dfn-cert: DFN-CERT-2015-0305  
dfn-cert: DFN-CERT-2015-0199  
dfn-cert: DFN-CERT-2015-0079  
dfn-cert: DFN-CERT-2015-0021  
dfn-cert: DFN-CERT-2014-1414  
dfn-cert: DFN-CERT-2013-1847  
dfn-cert: DFN-CERT-2013-1792  
dfn-cert: DFN-CERT-2012-1979  
dfn-cert: DFN-CERT-2012-1829  
dfn-cert: DFN-CERT-2012-1530  
dfn-cert: DFN-CERT-2012-1380  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
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

...continues on next page ...

...continued from previous page ...

```

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%****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.

... continues on next page ...

...continued from previous page ...

**Vulnerability Insight**

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1, Fingerprint2

**Vulnerability Detection Method**

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

OID:1.3.6.1.4.1.25623.1.0.105880

Version used: 2021-10-15T11:13:32Z

**References**

url: <https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**

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

**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

... continues on next page ...

...continued from previous page ...
<p>Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).</p> <p>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.</p>
<p><b>Vulnerability Insight</b></p> <p>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.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Checks the DHE temporary public key size.</p> <p>Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪...</p> <p>OID:1.3.6.1.4.1.25623.1.0.106223</p> <p>Version used: 2023-07-21T05:05:22Z</p>
<p><b>References</b></p> <p>url: <a href="https://weakdh.org/">https://weakdh.org/</a></p> <p>url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a></p>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<p><b>Summary</b></p> <p>The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size &lt; 2048).</p>
<b>Quality of Detection (QoD):</b> 80%
<p><b>Vulnerability Detection Result</b></p> <p>Server Temporary Key Size: 1024 bits</p>
<p><b>Impact</b></p> <p>An attacker might be able to decrypt the SSL/TLS communication offline.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Workaround</p> <p>Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).</p> <p>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.</p>
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2023-07-21T05:05:22Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

[ [return to 192.168.1.34](#) ]

### 2.1.17 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired
<b>Product detection result</b> 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)
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> 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
...continues on next page ...

...continued from previous page ...	
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
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.	
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> 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)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> 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
... continues on next page ...



...continued from previous page ...	
TLSv1.2	10
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> 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: 2024-07-24T05:06:37Z	
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013	
... continues on next page ...	

...continued from previous page ...

```
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: 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.

**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.

... continues on next page ...

...continued from previous page ...
Both CVEs are still kept in this VT as a reference to the origin of this flaw.
<b>Vulnerability Detection Method</b> 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: 2024-07-24T05:06:37Z
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112
Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
<b>Product detection result</b> 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)
<b>Summary</b> The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> ... continues on next page ...

...continued from previous page...																													
<p>The certificate of the remote service is signed by the following untrusted and/or dangerous CA:</p> <p>Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=California,C=US</p> <p>Certificate details:</p> <table><tr><td>fingerprint (SHA-1)</td><td>  4A5758F59279E82F2A913C83CA658D6964575A72</td></tr><tr><td>fingerprint (SHA-256)</td><td>  AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD</td></tr><tr><td colspan="2">5B23381002A885F556</td></tr><tr><td>issued by</td><td>  CN=localhost,OU=GlassFish,O=Oracle Corporation</td></tr><tr><td colspan="2">,L=Santa Clara,ST=California,C=US</td></tr><tr><td>public key algorithm</td><td>  RSA</td></tr><tr><td>public key size (bits)</td><td>  2048</td></tr><tr><td>serial</td><td>  04A9972F</td></tr><tr><td>signature algorithm</td><td>  sha256WithRSAEncryption</td></tr><tr><td>subject</td><td>  CN=localhost,OU=GlassFish,O=Oracle Corporation</td></tr><tr><td colspan="2">,L=Santa Clara,ST=California,C=US</td></tr><tr><td>subject alternative names (SAN)</td><td>  None</td></tr><tr><td>valid from</td><td>  2013-05-15 05:33:38 UTC</td></tr><tr><td>valid until</td><td>  2023-05-13 05:33:38 UTC</td></tr></table>		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
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																												
<p><b>Impact</b></p> <p>An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.</p>																													
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Replace the SSL/TLS certificate with one signed by a trusted CA.</p>																													
<p><b>Vulnerability Detection Method</b></p> <p>The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.</p> <p>Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.113054</p> <p>Version used: 2024-06-14T05:05:48Z</p>																													
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security</p> <p>Method: SSL/TLS: Collect and Report Certificate Details</p> <p>OID: 1.3.6.1.4.1.25623.1.0.103692)</p>																													
Medium (CVSS: 4.3)																													
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection																													
<p><b>Product detection result</b></p> <p>... continues on next page ...</p>																													

...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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.1 Method: SSL/TLS: Version Detection
...continues on next page ...

...continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389

cve: CVE-2015-0204

url: <https://ssl-config.mozilla.org/>url: <https://bettercrypto.org/>url: <https://datatracker.ietf.org/doc/rfc8996/>url: <https://vnhacker.blogspot.com/2011/09/beast.html>url: <https://web.archive.org/web/20201108095603/https://censys.io/blog/freak>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters>  
↔-report-2014

cert-bund: WID-SEC-2023-1435

cert-bund: CB-K18/0799

cert-bund: CB-K15/1751

cert-bund: CB-K15/1266

cert-bund: CB-K15/0850

cert-bund: CB-K15/0764

cert-bund: CB-K15/0720

cert-bund: CB-K15/0548

cert-bund: CB-K15/0526

cert-bund: CB-K15/0509

cert-bund: CB-K15/0493

cert-bund: CB-K15/0384

cert-bund: CB-K15/0365

cert-bund: CB-K15/0364

cert-bund: CB-K15/0302

cert-bund: CB-K15/0192

cert-bund: CB-K15/0079

cert-bund: CB-K15/0016

cert-bund: CB-K14/1342

cert-bund: CB-K14/0231

cert-bund: CB-K13/0845

cert-bund: CB-K13/0796

cert-bund: CB-K13/0790

dfn-cert: DFN-CERT-2020-0177

dfn-cert: DFN-CERT-2020-0111

dfn-cert: DFN-CERT-2019-0068

dfn-cert: DFN-CERT-2018-1441

dfn-cert: DFN-CERT-2018-1408

dfn-cert: DFN-CERT-2016-1372

dfn-cert: DFN-CERT-2016-1164

dfn-cert: DFN-CERT-2016-0388

dfn-cert: DFN-CERT-2015-1853

dfn-cert: DFN-CERT-2015-1332

dfn-cert: DFN-CERT-2015-0884

... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0800  
dfn-cert: DFN-CERT-2015-0758  
dfn-cert: DFN-CERT-2015-0567  
dfn-cert: DFN-CERT-2015-0544  
dfn-cert: DFN-CERT-2015-0530  
dfn-cert: DFN-CERT-2015-0396  
dfn-cert: DFN-CERT-2015-0375  
dfn-cert: DFN-CERT-2015-0374  
dfn-cert: DFN-CERT-2015-0305  
dfn-cert: DFN-CERT-2015-0199  
dfn-cert: DFN-CERT-2015-0079  
dfn-cert: DFN-CERT-2015-0021  
dfn-cert: DFN-CERT-2014-1414  
dfn-cert: DFN-CERT-2013-1847  
dfn-cert: DFN-CERT-2013-1792  
dfn-cert: DFN-CERT-2012-1979  
dfn-cert: DFN-CERT-2012-1829  
dfn-cert: DFN-CERT-2012-1530  
dfn-cert: DFN-CERT-2012-1380  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
dfn-cert: DFN-CERT-2012-0848  
dfn-cert: DFN-CERT-2012-0838  
dfn-cert: DFN-CERT-2012-0776  
dfn-cert: DFN-CERT-2012-0722  
dfn-cert: DFN-CERT-2012-0638  
dfn-cert: DFN-CERT-2012-0627  
dfn-cert: DFN-CERT-2012-0451  
dfn-cert: DFN-CERT-2012-0418  
dfn-cert: DFN-CERT-2012-0354  
dfn-cert: DFN-CERT-2012-0234  
dfn-cert: DFN-CERT-2012-0221  
dfn-cert: DFN-CERT-2012-0177  
dfn-cert: DFN-CERT-2012-0170  
dfn-cert: DFN-CERT-2012-0146  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126

...continues on next page ...

...continued from previous page ...

```

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 &lt; 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 (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**

... continues on next page ...



...continued from previous page ...
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
<b>Vulnerability Detection Method</b> 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: 2023-07-21T05:05:22Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> ... continues on next page ...

...continued from previous page ...
<p>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: 2023-07-21T05:05:22Z</p>
<p><b>References</b>  url: <a href="https://weakdh.org/">https://weakdh.org/</a>  url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a></p>

[\[ return to 192.168.1.34 \]](#)

### 2.1.18 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server Multiple Vulnerabilities - 02 - (Nov 2012) - Windows
<p><b>Product detection result</b>  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><b>Summary</b>  Oracle MySQL server is prone to multiple vulnerabilities.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b>  Installed version: 5.5.20  Fixed version:      Apply the patch</p>
<p><b>Impact</b>  Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).</p>
<p><b>Solution:</b>  <b>Solution type:</b> VendorFix  Apply the patch from the references or upgrade to latest version.</p>
<p><b>Affected Software/OS</b>  Oracle MySQL version 5.1.x to 5.1.65 and Oracle MySQL version 5.5.x to 5.5.27 on Windows.</p>
... continues on next page ...

...continued from previous page...
<b>Vulnerability Insight</b> The flaws are due to multiple unspecified errors in MySQL server component related to server installation and server optimizer.
<b>Vulnerability Detection Method</b> Details: Oracle MySQL Server Multiple Vulnerabilities - 02 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803112 Version used: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-3180 cve: CVE-2012-3177 cve: CVE-2012-3160 url: <a href="http://secunia.com/advisories/51008/">http://secunia.com/advisories/51008/</a> url: <a href="http://www.securityfocus.com/bid/56003">http://www.securityfocus.com/bid/56003</a> url: <a href="http://www.securityfocus.com/bid/56005">http://www.securityfocus.com/bid/56005</a> url: <a href="http://www.securityfocus.com/bid/56027">http://www.securityfocus.com/bid/56027</a> url: <a href="http://www.securelist.com/en/advisories/51008">http://www.securelist.com/en/advisories/51008</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html">http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html</a> url: <a href="https://support.oracle.com/rs?type=doc&amp;id=1475188.1">https://support.oracle.com/rs?type=doc&amp;id=1475188.1</a> dfn-cert: DFN-CERT-2012-2200 dfn-cert: DFN-CERT-2012-2118

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
...continues on next page...

...continued from previous page ...	
Fixed version:	5.5.29
Installation path / port:	3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.29 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5 through 5.5.28.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows OID: 1.3.6.1.4.1.25623.1.0.117205 Version used: 2021-02-12T11:09:59Z	
<b>Product Detection Result</b> 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)	
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL</a> advisory-id: cpujan2013 dfn-cert: DFN-CERT-2013-0259 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)

... continues on next page ...

...continued from previous page ...
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.24 Installation path / port: 3306/tcp
<b>Impact</b> The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'InnoDB' package / privilege.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.24 or later.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.x through 5.5.23.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows OID:1.3.6.1.4.1.25623.1.0.117267 Version used: 2021-03-18T11:53:07Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-1735 cve: CVE-2012-1757 cve: CVE-2012-1756 url: <a href="https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL</a> advisory-id: cpujul2012 dfn-cert: DFN-CERT-2012-1389

Medium (CVSS: 6.8)
NVT: MySQL Server Components Multiple Unspecified Vulnerabilities
<b>Product detection result</b> 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)
<b>Summary</b> MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20-log Fixed version: See advisory
<b>Impact</b> Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> MySQL version 5.1.x before 5.1.62 and 5.5.x before 5.5.22.
<b>Vulnerability Insight</b> Multiple unspecified errors exist in the Server Optimizer and Server DML components.
<b>Vulnerability Detection Method</b> Details: MySQL Server Components Multiple Unspecified Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.803808 Version used: 2023-07-27T05:05:08Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-1690
... continues on next page ...

...continued from previous page ...
cve: CVE-2012-1688 cve: CVE-2012-1703 url: <a href="http://secunia.com/advisories/48890">http://secunia.com/advisories/48890</a> url: <a href="http://www.securityfocus.com/bid/53058">http://www.securityfocus.com/bid/53058</a> url: <a href="http://www.securityfocus.com/bid/53067">http://www.securityfocus.com/bid/53067</a> url: <a href="http://www.securityfocus.com/bid/53074">http://www.securityfocus.com/bid/53074</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#AppendixMySQL">http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#AppendixMySQL</a> dfn-cert: DFN-CERT-2012-2118 dfn-cert: DFN-CERT-2012-1170 dfn-cert: DFN-CERT-2012-0939 dfn-cert: DFN-CERT-2012-0936 dfn-cert: DFN-CERT-2012-0933 dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.28 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.66, 5.5.28 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.65 and prior and 5.5 through 5.5.27.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
The flaw allows remote authenticated users to affect availability, related to GIS Extension.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.117201 Version used: 2021-02-12T11:09:59Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-5060 url: <a href="https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL</a> advisory-id: cpujan2013 dfn-cert: DFN-CERT-2013-0079

Medium (CVSS: 6.7)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote to have an impact on availability, confidentiality and integrity.
... continues on next page ...



...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.53 and earlier, 5.6.34 and earlier, 5.7.16 and earlier on Windows
<b>Vulnerability Insight</b> Multiple flaws exist due to: multiple unspecified errors in sub components 'Error Handling', 'Logging', 'MyISAM', 'Packaging', 'Optimizer', 'DML' and 'DDL'.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows OID:1.3.6.1.4.1.25623.1.0.809865 Version used: 2023-11-03T05:05:46Z
<b>Product Detection Result</b> 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)
<b>References</b> 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 cve: CVE-2017-3265 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html">http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html</a> url: <a href="http://www.securityfocus.com/bid/95571">http://www.securityfocus.com/bid/95571</a> url: <a href="http://www.securityfocus.com/bid/95560">http://www.securityfocus.com/bid/95560</a> url: <a href="http://www.securityfocus.com/bid/95491">http://www.securityfocus.com/bid/95491</a> url: <a href="http://www.securityfocus.com/bid/95527">http://www.securityfocus.com/bid/95527</a> url: <a href="http://www.securityfocus.com/bid/95565">http://www.securityfocus.com/bid/95565</a> url: <a href="http://www.securityfocus.com/bid/95588">http://www.securityfocus.com/bid/95588</a> url: <a href="http://www.securityfocus.com/bid/95501">http://www.securityfocus.com/bid/95501</a> url: <a href="http://www.securityfocus.com/bid/95585">http://www.securityfocus.com/bid/95585</a> url: <a href="http://www.securityfocus.com/bid/95520">http://www.securityfocus.com/bid/95520</a> cert-bund: CB-K18/0224 dfn-cert: DFN-CERT-2018-1276 dfn-cert: DFN-CERT-2018-0242
... continues on next page ...

...continued from previous page ...

```
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 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.

**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.

... continues on next page ...

...continued from previous page ...
Details: Oracle MySQL Security Update (cpujul2018 - 02) - Windows OID:1.3.6.1.4.1.25623.1.0.813706 Version used: 2023-11-03T16:10:08Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2018-2767 cve: CVE-2018-3066 cve: CVE-2018-3058 cve: CVE-2018-3070 url: <a href="https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL</a> 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 Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (cpuoct2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD): 80%</b>
... continues on next page ...

...continued from previous page...	
<b>Vulnerability Detection Result</b>	
Installed version:	5.5.20
Fixed version:	See the referenced vendor advisory
Installation	
path / port:	3306/tcp
<b>Impact</b>	
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.	
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
Updates are available. Please see the references for more information.	
<b>Affected Software/OS</b>	
Oracle MySQL Server versions 5.5.50 and prior, 5.6 through 5.6.31 and 5.7 through 5.7.13.	
<b>Vulnerability Insight</b>	
The flaw exists due to an unspecified error in the 'Server: DML' component.	
<b>Vulnerability Detection Method</b>	
Checks if a vulnerable version is present on the target host.	
Details: Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (. ↔..	
OID:1.3.6.1.4.1.25623.1.0.809374	
Version used: 2022-07-21T10:11:30Z	
<b>Product Detection Result</b>	
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)	
<b>References</b>	
cve: CVE-2016-5612	
url: <a href="https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL</a>	
advisory-id: cpuoct2016	
dfn-cert: DFN-CERT-2016-2089	
dfn-cert: DFN-CERT-2016-1859	
dfn-cert: DFN-CERT-2016-1849	
dfn-cert: DFN-CERT-2016-1790	
dfn-cert: DFN-CERT-2016-1714	

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.51 and prior.
<b>Vulnerability Insight</b> The flaw exists due to an unspecified error within the 'Server:DML' component.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows OID:1.3.6.1.4.1.25623.1.0.809378 Version used: 2022-07-21T10:11:30Z
<b>Product Detection Result</b> 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-2016-5624

url: <https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL>

advisory-id: cpuoct2016

dfn-cert: DFN-CERT-2016-1950

dfn-cert: DFN-CERT-2016-1790

dfn-cert: DFN-CERT-2016-1714

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server &lt;= 5.7.32 / 8.0 &lt;= 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 &lt;= 5.7.32 / 8.0 &lt;= 8.0.22 Security Update (cpuapr2021) - Wi.↵..

OID:1.3.6.1.4.1.25623.1.0.145794

Version used: 2023-10-20T16:09:12Z

**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)	
<b>References</b>	
cve: CVE-2020-1971	
cve: CVE-2021-2178	
cve: CVE-2021-2202	
url: <a href="https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL</a>	
advisory-id: cpuapr2021	
cert-bund: WID-SEC-2024-0794	
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	
...continues on next page ...	

...continued from previous page ...
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 <= 5.6.46 Security Update (cpujan2020) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified denial of service vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.47 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.47 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.46 and prior.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows OID:1.3.6.1.4.1.25623.1.0.143359 Version used: 2021-08-16T09:00:57Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2020-2579 url: <a href="https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.50 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.50, 5.7.32, 8.0.22 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.49 and prior, 5.7 through 5.7.31 and 8.0 through 8.0.21.
<b>Vulnerability Detection Method</b> 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 (↵.. ...continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.108959 Version used: 2021-08-16T12:00:57Z
<b>Product Detection Result</b> 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)
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL</a> advisory-id: cpuoct2020 cert-bund: CB-K20/1066 cert-bund: CB-K20/1017 dfn-cert: DFN-CERT-2021-2155 dfn-cert: DFN-CERT-2021-0002 dfn-cert: DFN-CERT-2020-2763 dfn-cert: DFN-CERT-2020-2756 dfn-cert: DFN-CERT-2020-2620 dfn-cert: DFN-CERT-2020-2380 dfn-cert: DFN-CERT-2020-2295

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 (May 2014) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page ...	
<b>Impact</b>	Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
	Apply the patch from the referenced advisory.
<b>Affected Software/OS</b>	Oracle MySQL version 5.5.36 and earlier and 5.6.16 and earlier on Windows.
<b>Vulnerability Insight</b>	Unspecified errors in the MySQL Server component via unknown vectors related to Performance Schema, Options, RBR.
<b>Vulnerability Detection Method</b>	Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Multiple Unspecified vulnerabilities - 02 (May 2014) - Windows OID:1.3.6.1.4.1.25623.1.0.804575 Version used: 2024-02-09T05:06:25Z
<b>Product Detection Result</b>	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)
<b>References</b>	cve: CVE-2014-2430 cve: CVE-2014-2431 cve: CVE-2014-2436 cve: CVE-2014-2440 url: <a href="http://secunia.com/advisories/57940">http://secunia.com/advisories/57940</a> url: <a href="http://www.securityfocus.com/bid/66850">http://www.securityfocus.com/bid/66850</a> url: <a href="http://www.securityfocus.com/bid/66858">http://www.securityfocus.com/bid/66858</a> url: <a href="http://www.securityfocus.com/bid/66890">http://www.securityfocus.com/bid/66890</a> url: <a href="http://www.securityfocus.com/bid/66896">http://www.securityfocus.com/bid/66896</a> url: <a href="http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638">http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html">http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html</a> cert-bund: CB-K14/0710 cert-bund: CB-K14/0464 cert-bund: CB-K14/0452 dfn-cert: DFN-CERT-2014-0742 dfn-cert: DFN-CERT-2014-0477 dfn-cert: DFN-CERT-2014-0459

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.30 Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.68, 5.5.30, 5.6.11 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.67 and prior, 5.5 through 5.5.29 and 5.6 through 5.6.10.
<b>Vulnerability Insight</b> Unspecified error in some unknown vectors related to Information Schema.
<b>Vulnerability Detection Method</b> 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: 2022-07-21T10:11:30Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-2378 cve: CVE-2013-1506 url: <a href="https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/59188">http://www.securityfocus.com/bid/59188</a> 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 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.30 Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.68, 5.5.30 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.67 and prior and 5.5 through 5.5.29.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
Unspecified error in Server Partition and in some unspecified vectors.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Wi. ↪.. OID:1.3.6.1.4.1.25623.1.0.117209 Version used: 2022-04-25T14:50:49Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-1521 cve: CVE-2013-1552 cve: CVE-2013-1555 cve: CVE-2012-5614 url: <a href="https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/59196">http://www.securityfocus.com/bid/59196</a> url: <a href="http://www.securityfocus.com/bid/59210">http://www.securityfocus.com/bid/59210</a> advisory-id: cpuapr2013 dfn-cert: DFN-CERT-2013-0839 dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation
... continues on next page ...

...continued from previous page ...	
path / port:	3306/tcp
<b>Impact</b>	Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b>	
<b>Solution type:</b> VendorFix	Updates are available. Please see the references for more information.
<b>Affected Software/OS</b>	Oracle MySQL Server versions 5.5.31 and prior and 5.6 through 5.6.11.
<b>Vulnerability Insight</b>	Unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b>	Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.806878 Version used: 2022-09-12T10:18:03Z
<b>Product Detection Result</b>	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)
<b>References</b>	cve: CVE-2016-0502 url: <a href="https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/81136">http://www.securityfocus.com/bid/81136</a> advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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 <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows	
<b>Product detection result</b>	
... 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.31 Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.69, 5.5.31, 5.6.11 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.68 and prior, 5.5 through 5.5.30 and 5.6 through 5.6.10.
<b>Vulnerability Insight</b> Unspecified error in Server Optimizer, Server Privileges, InnoDB, and in some unspecified vectors.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (. ↪.. OID:1.3.6.1.4.1.25623.1.0.117207 Version used: 2022-07-21T10:11:30Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-2375 cve: CVE-2013-1544
... continues on next page ...



...continued from previous page ...

```

cve: CVE-2013-1532
cve: CVE-2013-2389
cve: CVE-2013-2392
cve: CVE-2013-2391
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59207
url: http://www.securityfocus.com/bid/59209
url: http://www.securityfocus.com/bid/59224
url: http://www.securityfocus.com/bid/59242
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

```

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server &lt;= 5.5.38 / 5.6 &lt;= 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.

**Solution:**

**Solution type:** VendorFix  
Update to version 5.5.39, 5.6.20 or later.

**Affected Software/OS**

... continues on next page ...

...continued from previous page...	
Oracle MySQL Server versions 5.5.38 and prior and 5.6 through 5.6.19.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.804782 Version used: 2021-02-12T11:09:59Z	
<b>Product Detection Result</b> 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)	
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL</a> advisory-id: cpuoct2014 cert-bund: CB-K15/1518 cert-bund: CB-K15/0567 cert-bund: CB-K15/0415 cert-bund: CB-K14/1482 cert-bund: CB-K14/1420 cert-bund: CB-K14/1412 cert-bund: CB-K14/1299 dfn-cert: DFN-CERT-2015-1604 dfn-cert: DFN-CERT-2015-0593 dfn-cert: DFN-CERT-2015-0427 dfn-cert: DFN-CERT-2014-1567 dfn-cert: DFN-CERT-2014-1500 dfn-cert: DFN-CERT-2014-1489	
...continues on next page...	

...continued from previous page ...

dfn-cert: DFN-CERT-2014-1357  
 dfn-cert: DFN-CERT-2013-0259

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'

#### 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

... continues on next page ...

...continued from previous page ...	
Version used: 2023-11-03T05:05:46Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2017-10379 cve: CVE-2017-10384 cve: CVE-2017-10268 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html">http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html</a> url: <a href="http://www.securityfocus.com/bid/101415">http://www.securityfocus.com/bid/101415</a> url: <a href="http://www.securityfocus.com/bid/101406">http://www.securityfocus.com/bid/101406</a> url: <a href="http://www.securityfocus.com/bid/101390">http://www.securityfocus.com/bid/101390</a> cert-bund: CB-K18/0480 cert-bund: CB-K18/0242 cert-bund: CB-K18/0224 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 Multiple Unspecified vulnerabilities-02 (Jul 2014) - Windows	
<b>Product detection result</b> 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)	
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.	
... continues on next page ...	

...continued from previous page ...	
<b>Impact</b>	Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
	Apply the patch from the referenced advisory.
<b>Affected Software/OS</b>	
	Oracle MySQL version 5.5.37 and earlier and 5.6.17 and earlier on Windows.
<b>Vulnerability Insight</b>	
	Unspecified errors in the MySQL Server component via unknown vectors related to SRINFOSC and SRCHAR.
<b>Vulnerability Detection Method</b>	
	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: 2024-02-16T05:06:55Z
<b>Product Detection Result</b>	
	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)
<b>References</b>	
	cve: CVE-2014-4258 cve: CVE-2014-4260 url: <a href="http://secunia.com/advisories/59521">http://secunia.com/advisories/59521</a> url: <a href="http://www.securityfocus.com/bid/68564">http://www.securityfocus.com/bid/68564</a> url: <a href="http://www.securityfocus.com/bid/68573">http://www.securityfocus.com/bid/68573</a> url: <a href="http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_security_patches">http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_security_patches</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#AppendixMSQL">http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#AppendixMSQL</a> cert-bund: CB-K15/0567 cert-bund: CB-K14/1420 cert-bund: CB-K14/0891 cert-bund: CB-K14/0868 dfn-cert: DFN-CERT-2015-0593 dfn-cert: DFN-CERT-2014-1500 dfn-cert: DFN-CERT-2014-0930 dfn-cert: DFN-CERT-2014-0911

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation path / port:       3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to compromise availability of the system.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.11 and earlier on Windows.
<b>Vulnerability Insight</b> The flaw exists due to an error in 'Server: Optimizer'
<b>Vulnerability Detection Method</b> 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: 2023-07-25T05:05:58Z
<b>Product Detection Result</b> Product: cpe:/a:mysql:mysql:5.5.20-log Method: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.100152)
... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2017-10378  
 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  
 dfn-cert: DFN-CERT-2019-1047  
 dfn-cert: DFN-CERT-2018-1276  
 dfn-cert: DFN-CERT-2018-1265  
 dfn-cert: DFN-CERT-2018-0515  
 dfn-cert: DFN-CERT-2018-0260  
 dfn-cert: DFN-CERT-2018-0242  
 dfn-cert: DFN-CERT-2017-2137  
 dfn-cert: DFN-CERT-2017-1827

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server <= 5.6.44 / 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.
<b>Vulnerability Insight</b> Oracle MySQL Server is prone to multiple denial of service vulnerabilities. For further information refer to the official advisory via the referenced link.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (. ↔.. OID:1.3.6.1.4.1.25623.1.0.142645 Version used: 2023-10-27T16:11:32Z
<b>Product Detection Result</b> 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)
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.46 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.46, 5.7.28, 8.0.18 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.45 and prior, 5.7 through 5.7.27 and 8.0 through 8.0.17.
<b>Vulnerability Insight</b> Oracle MySQL Server is prone to multiple vulnerabilities. For further information refer to the official advisory via the referenced link.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (.↪.. OID:1.3.6.1.4.1.25623.1.0.143030 Version used: 2021-09-07T14:01:38Z
<b>Product Detection Result</b> 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-2019-2974  
 cve: CVE-2019-2911  
 url: <https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL>  
 advisory-id: cpuoct2019  
 cert-bund: CB-K20/1030  
 cert-bund: CB-K20/0109  
 cert-bund: CB-K19/0915  
 dfn-cert: DFN-CERT-2020-2763  
 dfn-cert: DFN-CERT-2020-2756  
 dfn-cert: DFN-CERT-2020-2620  
 dfn-cert: DFN-CERT-2020-2299  
 dfn-cert: DFN-CERT-2020-2180  
 dfn-cert: DFN-CERT-2020-1827  
 dfn-cert: DFN-CERT-2020-0658  
 dfn-cert: DFN-CERT-2020-0517  
 dfn-cert: DFN-CERT-2020-0103  
 dfn-cert: DFN-CERT-2019-2695  
 dfn-cert: DFN-CERT-2019-2687  
 dfn-cert: DFN-CERT-2019-2656  
 dfn-cert: DFN-CERT-2019-2301  
 dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 6.5)

NVT: Oracle MySQL Server &lt;= 5.1.66 / 5.5 &lt;= 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

**Solution:****Solution type:** VendorFix

... continues on next page ...

...continued from previous page ...	
Update to version 5.1.67, 5.5.29 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Wi. ↪.. OID:1.3.6.1.4.1.25623.1.0.803459 Version used: 2022-07-21T10:11:30Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2013-1531 url: <a href="https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL</a> advisory-id: cpuapr2013 dfn-cert: DFN-CERT-2013-0839 dfn-cert: DFN-CERT-2013-0798	

Medium (CVSS: 6.5)	
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows	
<b>Product detection result</b> 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)	
<b>Summary</b> Oracle MySQL is prone to multiple denial of service (DoS) vulnerabilities.	
<b>Quality of Detection (QoD): 80%</b>	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation	
... continues on next page ...	

...continued from previous page ...	
path / port:	3306/tcp
<b>Impact</b> Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.	
<b>Affected Software/OS</b> Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows	
<b>Vulnerability Insight</b> Multiple flaws exist due to: - An error in the 'Server: DDL' component. - Multiple errors in the 'Server: Optimizer' component.	
<b>Vulnerability Detection Method</b> 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: 2024-02-29T14:37:57Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2018-2668 cve: CVE-2018-2665 cve: CVE-2018-2622 cve: CVE-2018-2640 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html">http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html</a> 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	
... continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2018-0101

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

**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: 2024-02-09T05:06:25Z

**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)
<b>References</b> cve: CVE-2012-3147 cve: CVE-2012-3149 cve: CVE-2012-3144 url: <a href="http://secunia.com/advisories/51008/">http://secunia.com/advisories/51008/</a> url: <a href="http://www.securityfocus.com/bid/56006">http://www.securityfocus.com/bid/56006</a> url: <a href="http://www.securityfocus.com/bid/56008">http://www.securityfocus.com/bid/56008</a> url: <a href="http://www.securityfocus.com/bid/56022">http://www.securityfocus.com/bid/56022</a> url: <a href="http://www.securelist.com/en/advisories/51008">http://www.securelist.com/en/advisories/51008</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html">http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html</a> url: <a href="https://support.oracle.com/rs?type=doc&amp;id=1475188.1">https://support.oracle.com/rs?type=doc&amp;id=1475188.1</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a local unauthenticated vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.45 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.45, 5.7.27, 8.0.17 or later.
<b>Affected Software/OS</b>
... 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.
<b>Vulnerability Insight</b> Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (. ↪.. OID:1.3.6.1.4.1.25623.1.0.143032 Version used: 2021-09-08T08:01:40Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2019-2969 url: <a href="https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL</a> advisory-id: cpuoct2019 cert-bund: CB-K19/0915 dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 6.1)
NVT: Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (cpuapr2016v3) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation
... continues on next page ...

...continued from previous page...	
path / port:	3306/tcp
<b>Impact</b>	Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
	Updates are available. Please see the references for more information.
<b>Affected Software/OS</b>	Oracle MySQL Server versions 5.5.47 and prior, 5.6 through 5.6.28 and 5.7 through 5.7.10.
<b>Vulnerability Insight</b>	Unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b>	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: 2023-11-03T05:05:46Z
<b>Product Detection Result</b>	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)
<b>References</b>	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: <a href="https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL</a> advisory-id: cpuapr2016v3 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 Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.
<b>Vulnerability Insight</b> Unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.↵.. OID:1.3.6.1.4.1.25623.1.0.807924 Version used: 2023-11-03T05:05:46Z
<b>Product Detection Result</b> 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)
<b>References</b> 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: <a href="https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMySQL">https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMySQL</a> advisory-id: cpuapr2016v3 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: 5.9)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a vulnerability in a third party library.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> ... continues on next page ...

...continued from previous page...	
The flaw makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.	
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.117194 Version used: 2022-08-31T10:10:28Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2015-7744 url: <a href="https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL</a> advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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	
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.43 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.43, 5.7.25, 8.0.14 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (. ↪.. OID:1.3.6.1.4.1.25623.1.0.142405 Version used: 2021-09-07T14:01:38Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2018-3123 url: <a href="https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.44 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.44, 5.7.26, 8.0.16 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.43 and prior, 5.7 through 5.7.25 and 8.0 through 8.0.15.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (.↪.. OID:1.3.6.1.4.1.25623.1.0.142403 Version used: 2022-03-28T03:06:01Z
<b>Product Detection Result</b> 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-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-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  
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

... continues on next page ...

...continued from previous page ...

```

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

```

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**

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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Oracle MySQL Server 5.7.2 and earlier on Windows.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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: 2024-02-16T05:06:55Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-3152 url: <a href="http://www.ocert.org/advisories/ocert-2015-003.html">http://www.ocert.org/advisories/ocert-2015-003.html</a> url: <a href="https://duo.com/blog/backronym-mysql-vulnerability">https://duo.com/blog/backronym-mysql-vulnerability</a> cert-bund: CB-K18/0871 cert-bund: CB-K15/1045 cert-bund: CB-K15/1042 cert-bund: CB-K15/1020 cert-bund: CB-K15/0994 cert-bund: CB-K15/0964 cert-bund: CB-K15/0895 dfn-cert: DFN-CERT-2016-1004 dfn-cert: DFN-CERT-2015-1105 dfn-cert: DFN-CERT-2015-1096 dfn-cert: DFN-CERT-2015-1071 dfn-cert: DFN-CERT-2015-1051 dfn-cert: DFN-CERT-2015-1016 dfn-cert: DFN-CERT-2015-0942
Medium (CVSS: 5.9) NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Windows
<b>Product detection result</b> <code>cpe:/a:mysql:mysql:5.5.20-log</code>
... 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)
<b>Summary</b> Oracle MySQL Server is prone to a unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.43 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.43, 8.0.34 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.
<b>Vulnerability Detection Method</b> 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 (cpujul2023) - Win. ↪.. OID:1.3.6.1.4.1.25623.1.0.149981 Version used: 2023-10-13T05:06:10Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2023-22053 url: <a href="https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL</a> advisory-id: cpujul2023 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-1794 dfn-cert: DFN-CERT-2024-1188 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: 5.7)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 (Apr 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation path / port:       3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to cause a denial of service.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Server : Optimizer, DDL, Server : Compiling, Server : Federated.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> Product: cpe:/a:mysql:mysql:5.5.20-log Method: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.100152)
... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2015-2571  
 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  
 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 &lt;= 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%

... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow local users to affect availability.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.46 and prior.
<b>Vulnerability Insight</b> Unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Optimizer'.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows OID:1.3.6.1.4.1.25623.1.0.807922 Version used: 2022-08-31T10:10:28Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-0651 url: <a href="https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL</a> advisory-id: cpuapr2016v3 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: 5.4)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.29 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.67, 5.5.29 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.
<b>Vulnerability Detection Method</b> 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: 2023-11-02T05:05:26Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-5611 cve: CVE-2013-0384 cve: CVE-2013-0389 cve: CVE-2013-0385 ... continues on next page ...

...continued from previous page ...

```

cve: CVE-2013-0375
cve: CVE-2012-1702
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#AppendixMSQL
advisory-id: cpujan2013
cert-bund: CB-K13/0919
cert-bund: CB-K13/0603
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1597
dfn-cert: DFN-CERT-2013-0259
dfn-cert: DFN-CERT-2013-0192
dfn-cert: DFN-CERT-2013-0119
dfn-cert: DFN-CERT-2013-0118
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2013-0079
dfn-cert: DFN-CERT-2013-0037
dfn-cert: DFN-CERT-2013-0028
dfn-cert: DFN-CERT-2012-2285
dfn-cert: DFN-CERT-2012-2258
dfn-cert: DFN-CERT-2012-2215
dfn-cert: DFN-CERT-2012-2200

```

Medium (CVSS: 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

... continues on next page ...

...continued from previous page ...	
path / port:	3306/tcp
<b>Impact</b>	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.
<b>Solution:</b>	
<b>Solution type:</b>	VendorFix
	Apply the patch from the referenced advisory.
<b>Affected Software/OS</b>	Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier on Windows
<b>Vulnerability Insight</b>	The flaw exists due to an incorrect implementation or enforcement of 'ssl-mode=REQUIRED' in MySQL.
<b>Vulnerability Detection Method</b>	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: 2023-07-25T05:05:58Z
<b>Product Detection Result</b>	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)
<b>References</b>	cve: CVE-2017-3305 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html">http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html</a> url: <a href="http://www.securityfocus.com/bid/97023">http://www.securityfocus.com/bid/97023</a> 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 <= 5.7.39 / 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.

... continues on next page ...

...continued from previous page ...	
↔25623.1.0.100152)	
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.40 Installation path / port: 3306/tcp	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.40, 8.0.31 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.30.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.118388 Version used: 2022-10-24T10:14:58Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2022-2097 cve: CVE-2022-21617 cve: CVE-2022-21608 url: <a href="https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL</a> 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	
... continues on next page ...	



...continued from previous page ...

```

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 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**

... continues on next page ...

...continued from previous page ...
<b>Installed version:</b> 5.5.20 <b>Fixed version:</b> Apply the patch
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, 5.7.18 and earlier, on Windows
<b>Vulnerability Insight</b> Multiple flaws exist due to <ul style="list-style-type: none"> <li>- A flaw in the Client mysqldump component.</li> <li>- A flaw in the Server: DDL component.</li> <li>- A flaw in the C API component.</li> <li>- A flaw in the Connector/C component.</li> <li>- A flaw in the Server: Charsets component.</li> </ul>
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows OID:1.3.6.1.4.1.25623.1.0.811432 Version used: 2024-02-29T14:37:57Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2017-3651 cve: CVE-2017-3653 cve: CVE-2017-3652 cve: CVE-2017-3635 cve: CVE-2017-3648 cve: CVE-2017-3641 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html">http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html</a> ↪#AppendixMSQL url: <a href="http://www.securityfocus.com/bid/99802">http://www.securityfocus.com/bid/99802</a> url: <a href="http://www.securityfocus.com/bid/99810">http://www.securityfocus.com/bid/99810</a> url: <a href="http://www.securityfocus.com/bid/99805">http://www.securityfocus.com/bid/99805</a>
... continues on next page ...

...continued from previous page ...
url: <a href="http://www.securityfocus.com/bid/99730">http://www.securityfocus.com/bid/99730</a>
url: <a href="http://www.securityfocus.com/bid/99789">http://www.securityfocus.com/bid/99789</a>
url: <a href="http://www.securityfocus.com/bid/99767">http://www.securityfocus.com/bid/99767</a>
cert-bund: CB-K18/0224
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.46 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.46, 5.7.28 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.45 and prior and 5.7 through 5.7.27.
<b>Vulnerability Insight</b> Oracle MySQL Server is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...
For further information refer to the official advisory via the referenced link.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Wi. ↪.. OID:1.3.6.1.4.1.25623.1.0.143034 Version used: 2021-09-08T08:01:40Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2019-2922 cve: CVE-2019-2923 cve: CVE-2019-2924 cve: CVE-2019-2910 url: <a href="https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL</a> 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 Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.47 Installation
... continues on next page ...

...continued from previous page ...	
path / port:	3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.47, 5.7.27 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.46 and prior and 5.7 through 5.7.26.	
<b>Vulnerability Detection Method</b> 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: 2021-08-16T09:00:57Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2019-1547 cve: CVE-2019-1549 cve: CVE-2019-1552 cve: CVE-2019-1563 url: <a href="https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL</a> 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 cert-bund: CB-K20/1016 cert-bund: CB-K20/0321 cert-bund: CB-K20/0318 cert-bund: CB-K20/0043 cert-bund: CB-K20/0038 cert-bund: CB-K20/0036 cert-bund: CB-K20/0028 cert-bund: CB-K19/1025 cert-bund: CB-K19/0919 cert-bund: CB-K19/0915 cert-bund: CB-K19/0808	
...continues on next page ...	

...continued from previous page ...
cert-bund: CB-K19/0675 dfn-cert: DFN-CERT-2023-2709 dfn-cert: DFN-CERT-2020-2014 dfn-cert: DFN-CERT-2020-1729 dfn-cert: DFN-CERT-2020-0895 dfn-cert: DFN-CERT-2020-0776 dfn-cert: DFN-CERT-2020-0775 dfn-cert: DFN-CERT-2020-0772 dfn-cert: DFN-CERT-2020-0716 dfn-cert: DFN-CERT-2020-0277 dfn-cert: DFN-CERT-2020-0101 dfn-cert: DFN-CERT-2020-0096 dfn-cert: DFN-CERT-2020-0091 dfn-cert: DFN-CERT-2020-0090 dfn-cert: DFN-CERT-2019-2164 dfn-cert: DFN-CERT-2019-2149 dfn-cert: DFN-CERT-2019-1900 dfn-cert: DFN-CERT-2019-1897 dfn-cert: DFN-CERT-2019-1559

Medium (CVSS: 5.3)

NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

#### Product detection result

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

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)

#### Summary

Oracle MySQL is prone to vulnerability.

**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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, on Windows
<b>Vulnerability Insight</b> The flaw exists due to an error in the Client programs component.
<b>Vulnerability Detection Method</b> 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: 2024-02-29T14:37:57Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2017-3636 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html">http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html</a> ↪#AppendixMSQL url: <a href="http://www.securityfocus.com/bid/99736">http://www.securityfocus.com/bid/99736</a> cert-bund: CB-K18/0224 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: 5.0) NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 (Apr 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> ... continues on next page ...

...continued from previous page ...
Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to cause a denial of service.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier on windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to DDL, Server : Security : Privileges, Server : Security : Encryption, InnoDB : DML.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-2573 cve: CVE-2015-2568 cve: CVE-2015-0441 cve: CVE-2015-0433 url: <a href="http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html">http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html</a> url: <a href="http://www.securityfocus.com/bid/74078">http://www.securityfocus.com/bid/74078</a> url: <a href="http://www.securityfocus.com/bid/74073">http://www.securityfocus.com/bid/74073</a> url: <a href="http://www.securityfocus.com/bid/74103">http://www.securityfocus.com/bid/74103</a> url: <a href="http://www.securityfocus.com/bid/74089">http://www.securityfocus.com/bid/74089</a>
... continues on next page ...



...continued from previous page ...
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
<b>Product detection result</b> 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)
<b>Summary</b> MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b>
... continues on next page ...

...continued from previous page ...
Oracle MySQL 5.5.30 and earlier and 5.6.10 on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Prepared Statements, Server Options and Server Partition.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-3801 cve: CVE-2013-3805 cve: CVE-2013-3794 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html">http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html</a> url: <a href="http://www.securityfocus.com/bid/61222">http://www.securityfocus.com/bid/61222</a> url: <a href="http://www.securityfocus.com/bid/61256">http://www.securityfocus.com/bid/61256</a> url: <a href="http://www.securityfocus.com/bid/61269">http://www.securityfocus.com/bid/61269</a> cert-bund: CB-K13/0919 cert-bund: CB-K13/0620 dfn-cert: DFN-CERT-2013-1937 dfn-cert: DFN-CERT-2013-1599 dfn-cert: DFN-CERT-2013-1553 dfn-cert: DFN-CERT-2013-1478
Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.43, 8.x <= 8.0.31 Security Update (cpuoct2023) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to denial of service (DoS) vulnerability.
... continues on next page ...

...continued from previous page ...	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.44 Installation path / port: 3306/tcp	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.44, 8.0.32 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.43 and prior and 8.x through 8.0.31.	
<b>Vulnerability Detection Method</b> 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: 2023-10-20T05:06:03Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2023-22028 url: <a href="https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL</a> 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 <= 5.7.42, 8.x <= 8.0.31 Security Update (cpuoct2023) - Windows
<b>Product detection result</b> 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 ...
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.43 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.43, 8.0.32 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.31.
<b>Vulnerability Detection Method</b> 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: 2023-10-20T05:06:03Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2023-22015 cve: CVE-2023-22026 url: <a href="https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixMSQL</a> advisory-id: cpuoct2023 cert-bund: WID-SEC-2023-2690 dfn-cert: DFN-CERT-2023-2536

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.41 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.41 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.40 and prior.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows OID:1.3.6.1.4.1.25623.1.0.149168 Version used: 2023-10-13T05:06:10Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2023-21840 url: <a href="https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL</a> advisory-id: cpujan2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1424
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0126 dfn-cert: DFN-CERT-2023-0105
Medium (CVSS: 4.9) NVT: Oracle MySQL Security Update (cpujul2018 - 04) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See reference Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.
<b>Solution:</b> <b>Solution type:</b> VendorFix The vendor has released updates. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.60 and earlier.
<b>Vulnerability Insight</b> Multiple flaws exist due to an error in the 'Server: Security: Privileges' component of MySQL Server.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Security Update (cpujul2018 - 04) - Windows OID:1.3.6.1.4.1.25623.1.0.813710 Version used: 2022-08-22T10:11:10Z
... continues on next page ...

...continued from previous page ...
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2018-3063 url: <a href="https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL</a> 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

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server Component 'Replication' Unspecified vulnerability (Oct 2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
... continues on next page ...

...continued from previous page ...	
<b>Affected Software/OS</b> Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows	
<b>Vulnerability Insight</b> Unspecified error in the MySQL Server component via unknown vectors related to Replication.	
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2013-5807 url: <a href="http://secunia.com/advisories/55327">http://secunia.com/advisories/55327</a> url: <a href="http://www.securityfocus.com/bid/63105">http://www.securityfocus.com/bid/63105</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html">http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html</a> cert-bund: CB-K14/0187 cert-bund: CB-K13/1072 cert-bund: CB-K13/0840 cert-bund: CB-K13/0789 dfn-cert: DFN-CERT-2014-0190 dfn-cert: DFN-CERT-2013-2099 dfn-cert: DFN-CERT-2013-1846 dfn-cert: DFN-CERT-2013-1795	

Medium (CVSS: 4.9)	
NVT: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows	
<b>Product detection result</b> 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)	
<b>Summary</b> ... continues on next page ...	



...continued from previous page ...
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.34 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.34 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.33 and prior.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows OID:1.3.6.1.4.1.25623.1.0.145802 Version used: 2021-08-26T13:01:12Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2021-2154 url: <a href="https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL</a> advisory-id: cpuapr2021 cert-bund: WID-SEC-2023-0065 cert-bund: CB-K21/0421 dfn-cert: DFN-CERT-2022-1241 dfn-cert: DFN-CERT-2022-0933 dfn-cert: DFN-CERT-2022-0666 dfn-cert: DFN-CERT-2021-1660 dfn-cert: DFN-CERT-2021-0984 dfn-cert: DFN-CERT-2021-0821

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.31 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.31, 8.0.18 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.30 and prior and 8.0 through 8.0.17.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Wi. ↵.. OID:1.3.6.1.4.1.25623.1.0.145804 Version used: 2021-08-26T13:01:12Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2021-2160 url: <a href="https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMySQL">https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMySQL</a> advisory-id: cpuapr2021 cert-bund: WID-SEC-2023-0065
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K21/0421  
dfn-cert: DFN-CERT-2021-0821

Medium (CVSS: 4.9)

NVT: Oracle MySQL Server &lt;= 5.7.41, 8.x &lt;= 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

**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: 2023-10-13T05:06:10Z

**Product Detection Result**

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

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

... continues on next page ...

...continued from previous page ...
cve: CVE-2023-22007 url: <a href="https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL</a> 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 <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpu-jan2021) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.51 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.51, 5.7.33, 8.0.23 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.32 and 8.0 through 8.0.22.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (.↵.. OID:1.3.6.1.4.1.25623.1.0.145224 Version used: 2021-08-26T13:01:12Z
... continues on next page ...

...continued from previous page ...
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2021-2022 cve: CVE-2021-2060 url: <a href="https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.51 Installation path / port: 3306/tcp
<b>Impact</b> Successful attacks of this vulnerability can result in the unauthorized ability to cause a hang or frequently repeatedly crash (complete DOS) the MySQL Server.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.51, 5.7.31, 8.0.18 or later.
... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.30 and 8.0 through 8.0.17.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (. ↔.. OID:1.3.6.1.4.1.25623.1.0.145222 Version used: 2021-08-26T13:01:12Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2021-2001 url: <a href="https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL</a> 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: 4.6)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
...continues on next page ...

...continued from previous page ...	
Fixed version:	5.5.30
Installation path / port:	3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.30, 5.6.11 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5 through 5.5.29 and 5.6 through 5.6.10.	
<b>Vulnerability Detection Method</b> 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: 2021-02-12T11:09:59Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2013-1523 url: <a href="https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL</a> advisory-id: cpuapr2013 dfn-cert: DFN-CERT-2013-0798	

Medium (CVSS: 4.4)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
... continues on next page ...

...continued from previous page...	
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:     Apply the patch Installation path / port:       3306/tcp	
<b>Impact</b> Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.	
<b>Affected Software/OS</b> Oracle MySQL version 5.5.53 and earlier on Windows	
<b>Vulnerability Insight</b> The flaw exists due to an unspecified error in sub component 'Server: Charsets'.	
<b>Vulnerability Detection Method</b> 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: 2023-07-25T05:05:58Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2017-3243 url: <a href="http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html">http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html</a> url: <a href="http://www.securityfocus.com/bid/95538">http://www.securityfocus.com/bid/95538</a> cert-bund: CB-K18/0224 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.37 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.37, 8.0.28 or later.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.
<b>Vulnerability Detection Method</b> 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: 2023-10-19T05:05:21Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2022-21595 url: <a href="https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMySQL">https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMySQL</a> advisory-id: cpuoct2022 cert-bund: WID-SEC-2024-1591 ... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2022-1776 dfn-cert: DFN-CERT-2023-0504 dfn-cert: DFN-CERT-2022-2306
Medium (CVSS: 4.3) NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 (Jul 2015)
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect confidentiality via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier on Windows
<b>Vulnerability Insight</b> Unspecified errors exist in the MySQL Server component via unknown vectors related to Server : Pluggable Auth and Server : Security : Privileges.
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-02-20T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> 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 <= 8.0.16 Security Update (cpuoct2022) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.7.40 Installation path / port: 3306/tcp
... continues on next page ...

...continued from previous page...	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.40, 8.0.17 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.16.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Wi. ↔.. OID:1.3.6.1.4.1.25623.1.0.118384 Version used: 2023-10-19T05:05:21Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2022-21589 url: <a href="https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL</a> 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: 4.3)	
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Windows	
<b>Product detection result</b> 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)	
<b>Summary</b> Oracle MySQL Server is prone to an information disclosure vulnerability.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> ... continues on next page ...	

...continued from previous page ...	
Installed version:	5.5.20
Fixed version:	5.7.40
Installation path / port:	3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.7.40, 8.0.30 or later.	
<b>Affected Software/OS</b> Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.29.	
<b>Vulnerability Detection Method</b> 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: 2023-10-19T05:05:21Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2022-21592 url: <a href="https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL</a> 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: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> 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 ...
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.31 Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.31, 5.6.11 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.10.
<b>Vulnerability Insight</b> Unspecified error in some unknown vectors related to Stored Procedure.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) . ↔.. OID:1.3.6.1.4.1.25623.1.0.809815 Version used: 2022-04-25T14:50:49Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-2376 cve: CVE-2013-1511 url: <a href="https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/59227">http://www.securityfocus.com/bid/59227</a> advisory-id: cpuapr2013 dfn-cert: DFN-CERT-2013-0882 dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability (Oct 2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> 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.
<b>Vulnerability Insight</b> Unspecified error in the MySQL Server component via unknown vectors related to Optimizer.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z
<b>Product Detection Result</b> Product: cpe:/a:mysql:mysql:5.5.20-log Method: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.100152)
... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2013-3839  
 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**

... continues on next page ...



...continued from previous page ...
Oracle MySQL version 5.1.x to 5.1.63 and Oracle MySQL version 5.5.x to 5.5.25 on Windows.
<b>Vulnerability Insight</b> The flaws are due to multiple unspecified errors in MySQL server component vectors related to InnoDB plugin, server full text search and InnoDB.
<b>Vulnerability Detection Method</b> Details: Oracle MySQL Server Multiple Vulnerabilities - 03 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803113 Version used: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> 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 <= 5.5.46 Security Update (cpujan2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD): 80%</b>
... continues on next page ...

...continued from previous page...	
<b>Vulnerability Detection Result</b>	<p>Installed version: 5.5.20</p> <p>Fixed version: See the referenced vendor advisory</p> <p>Installation path / port: 3306/tcp</p>
<b>Impact</b>	<p>Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.</p>
<b>Solution:</b>	<p><b>Solution type:</b> VendorFix</p> <p>Updates are available. Please see the references for more information.</p>
<b>Affected Software/OS</b>	<p>Oracle MySQL Server versions 5.5.46 and prior.</p>
<b>Vulnerability Insight</b>	<p>Unspecified errors exist in the 'MySQL Server' component via unknown vectors.</p>
<b>Vulnerability Detection Method</b>	<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Oracle MySQL Server &lt;= 5.5.46 Security Update (cpujan2016) - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.117190</p> <p>Version used: 2021-02-12T11:09:59Z</p>
<b>Product Detection Result</b>	<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>
<b>References</b>	<p>cve: CVE-2016-0616</p> <p>url: <a href="https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL</a></p> <p>advisory-id: cpujan2016</p> <p>cert-bund: WID-SEC-2024-1482</p> <p>dfn-cert: DFN-CERT-2016-1192</p> <p>dfn-cert: DFN-CERT-2016-0994</p> <p>dfn-cert: DFN-CERT-2016-0845</p> <p>dfn-cert: DFN-CERT-2016-0532</p> <p>dfn-cert: DFN-CERT-2016-0266</p> <p>dfn-cert: DFN-CERT-2016-0265</p> <p>dfn-cert: DFN-CERT-2016-0143</p> <p>dfn-cert: DFN-CERT-2016-0104</p>

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.46 and prior and 5.6 through 5.6.27.
<b>Vulnerability Insight</b> Unspecified errors exist in the 'MySQL Server' component via unknown vectors.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Wi. ↵.. OID:1.3.6.1.4.1.25623.1.0.806877 Version used: 2022-04-13T13:17:10Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-0596 url: <a href="https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMySQL">https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMySQL</a> url: <a href="http://www.securityfocus.com/bid/81176">http://www.securityfocus.com/bid/81176</a> url: <a href="http://www.securityfocus.com/bid/81198">http://www.securityfocus.com/bid/81198</a> url: <a href="http://www.securityfocus.com/bid/81130">http://www.securityfocus.com/bid/81130</a> advisory-id: cpujan2016 cert-bund: WID-SEC-2024-1482 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 <= 5.5.38 Security Update (cpuoct2014) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.39 Installation path / port: 3306/tcp
<b>Impact</b> ... continues on next page ...

...continued from previous page...
Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.39 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.38 and prior.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to SERVER:DDL.
<b>Vulnerability Detection Method</b> 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: 2022-04-14T11:24:11Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2014-6520 url: <a href="https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/70510">http://www.securityfocus.com/bid/70510</a> 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: MySQL Server Component Partition Unspecified Vulnerability
<b>Product detection result</b> 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)
<b>Summary</b> MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20-log Fixed version: 5.5.22
<b>Impact</b> Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> MySQL version 5.5.x before 5.5.22
<b>Vulnerability Insight</b> Unspecified error in MySQL Server component related to Partition.
<b>Vulnerability Detection Method</b> Details: MySQL Server Component Partition Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.803801 Version used: 2024-03-04T14:37:58Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-1697
... continues on next page ...

...continued from previous page ...

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: 1.3.6.1.4.1.1.25623.1.0.100152)

**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.

**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

... continues on next page ...

...continued from previous page ...
Version used: 2024-02-16T05:06:55Z
<b>Product Detection Result</b> 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)
<b>References</b> 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#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: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 (Jul 2015)
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation
... continues on next page ...



...continued from previous page ...	
path / port:	3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to cause denial-of-service attack.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.	
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on Windows.	
<b>Vulnerability Insight</b> Unspecified errors exist in the MySQL Server component via unknown vectors related to DML, Server : I_S, Server : Optimizer, and GIS.	
<b>Vulnerability Detection Method</b> 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: 2024-02-20T05:05:48Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2015-2648 cve: CVE-2015-4752 cve: CVE-2015-2643 cve: CVE-2015-2582 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html">http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html</a> url: <a href="http://www.securityfocus.com/bid/75822">http://www.securityfocus.com/bid/75822</a> url: <a href="http://www.securityfocus.com/bid/75849">http://www.securityfocus.com/bid/75849</a> url: <a href="http://www.securityfocus.com/bid/75830">http://www.securityfocus.com/bid/75830</a> url: <a href="http://www.securityfocus.com/bid/75751">http://www.securityfocus.com/bid/75751</a> 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	
... continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2015-1071

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%**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: 2024-02-09T05:06:25Z

**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)
<b>References</b> cve: CVE-2015-0432 url: <a href="http://secunia.com/advisories/62525">http://secunia.com/advisories/62525</a> url: <a href="http://www.securityfocus.com/bid/72217">http://www.securityfocus.com/bid/72217</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html">http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html</a> cert-bund: CB-K15/1193 cert-bund: CB-K15/0964 cert-bund: CB-K15/0567 cert-bund: CB-K15/0415 cert-bund: CB-K15/0073 dfn-cert: DFN-CERT-2015-1264 dfn-cert: DFN-CERT-2015-1016 dfn-cert: DFN-CERT-2015-0593 dfn-cert: DFN-CERT-2015-0427 dfn-cert: DFN-CERT-2015-0074

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 (Oct 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation path / port:       3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix
... continues on next page ...

...continued from previous page ...
Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier on windows
<b>Vulnerability Insight</b> Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-4913 cve: CVE-2015-4830 cve: CVE-2015-4826 cve: CVE-2015-4815 cve: CVE-2015-4807 cve: CVE-2015-4802 cve: CVE-2015-4792 cve: CVE-2015-4870 cve: CVE-2015-4861 cve: CVE-2015-4858 cve: CVE-2015-4836 url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html">http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html</a> url: <a href="http://www.securityfocus.com/bid/77153">http://www.securityfocus.com/bid/77153</a> url: <a href="http://www.securityfocus.com/bid/77228">http://www.securityfocus.com/bid/77228</a> url: <a href="http://www.securityfocus.com/bid/77237">http://www.securityfocus.com/bid/77237</a> url: <a href="http://www.securityfocus.com/bid/77222">http://www.securityfocus.com/bid/77222</a> url: <a href="http://www.securityfocus.com/bid/77205">http://www.securityfocus.com/bid/77205</a> url: <a href="http://www.securityfocus.com/bid/77165">http://www.securityfocus.com/bid/77165</a> url: <a href="http://www.securityfocus.com/bid/77171">http://www.securityfocus.com/bid/77171</a> url: <a href="http://www.securityfocus.com/bid/77208">http://www.securityfocus.com/bid/77208</a> url: <a href="http://www.securityfocus.com/bid/77137">http://www.securityfocus.com/bid/77137</a> url: <a href="http://www.securityfocus.com/bid/77145">http://www.securityfocus.com/bid/77145</a> url: <a href="http://www.securityfocus.com/bid/77190">http://www.securityfocus.com/bid/77190</a> cert-bund: WID-SEC-2024-1483 cert-bund: CB-K15/1844
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1600  
 cert-bund: CB-K15/1554  
 dfn-cert: DFN-CERT-2016-1192  
 dfn-cert: DFN-CERT-2016-0845  
 dfn-cert: DFN-CERT-2016-0695  
 dfn-cert: DFN-CERT-2016-0532  
 dfn-cert: DFN-CERT-2016-0266  
 dfn-cert: DFN-CERT-2016-0265  
 dfn-cert: DFN-CERT-2015-1946  
 dfn-cert: DFN-CERT-2015-1692  
 dfn-cert: DFN-CERT-2015-1638

Medium (CVSS: 4.0)

NVT: Oracle MySQL Server &lt;= 5.1.62 / 5.4.x &lt;= 5.5.22 Security Update (cpujul2012) - Windows

**Product detection result**

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

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)

**Summary**

Oracle MySQL Server is prone to an unspecified vulnerability.

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

Installed version: 5.5.20

Fixed version: 5.5.23

Installation

path / port: 3306/tcp

**Impact**

The flaw allows remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' package / privilege.

**Solution:****Solution type:** VendorFix

Update to version 5.1.63, 5.5.23 or later.

**Affected Software/OS**

Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.

... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - . ↔.. OID:1.3.6.1.4.1.25623.1.0.117263 Version used: 2021-03-18T11:53:07Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-1689 url: <a href="https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL</a> 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.24 Installation path / port: 3306/tcp
<b>Impact</b> The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'GIS Extension' package / privilege.
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.1.63, 5.5.24 or later.
<b>Affected Software/OS</b> Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.23.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - . ↔.. OID:1.3.6.1.4.1.25623.1.0.117265 Version used: 2021-03-18T11:53:07Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2012-0540 cve: CVE-2012-1734 cve: CVE-2012-2749 url: <a href="https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL</a> 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 Multiple Unspecified Vulnerabilities-08 (Oct 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.44 and earlier on windows
<b>Vulnerability Insight</b> Unspecified error exists in the MySQL Server component via unknown vectors related to Server.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-4816 url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html">http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html</a> url: <a href="http://www.securityfocus.com/bid/77134">http://www.securityfocus.com/bid/77134</a> cert-bund: WID-SEC-2024-1483 cert-bund: CB-K15/1844 cert-bund: CB-K15/1600 cert-bund: CB-K15/1554 dfn-cert: DFN-CERT-2016-1192 dfn-cert: DFN-CERT-2016-0845 dfn-cert: DFN-CERT-2016-0532 dfn-cert: DFN-CERT-2016-0266 dfn-cert: DFN-CERT-2015-1946 dfn-cert: DFN-CERT-2015-1692
... continues on next page ...



...continued from previous page ...
dfn-cert: DFN-CERT-2015-1638
Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 (Feb 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
<b>Impact</b> Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to DLL.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> Product: cpe:/a:mysql:mysql:5.5.20-log Method: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.100152
... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2015-0391  
 url: <http://secunia.com/advisories/62525>  
 url: <http://www.securityfocus.com/bid/72205>  
 url: <http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html>  
 cert-bund: CB-K15/1193  
 cert-bund: CB-K15/0567  
 cert-bund: CB-K15/0415  
 cert-bund: CB-K15/0073  
 dfn-cert: DFN-CERT-2015-1264  
 dfn-cert: DFN-CERT-2015-0593  
 dfn-cert: DFN-CERT-2015-0427  
 dfn-cert: DFN-CERT-2015-0074

Medium (CVSS: 4.0)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 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)

**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**

... continues on next page ...

...continued from previous page ...
Unspecified errors in the MySQL Server component via unknown vectors related to Optimizer, InnoDB, and Locking.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2014-0386 cve: CVE-2014-0393 cve: CVE-2014-0402 url: <a href="http://secunia.com/advisories/56491">http://secunia.com/advisories/56491</a> url: <a href="http://www.securityfocus.com/bid/64877">http://www.securityfocus.com/bid/64877</a> url: <a href="http://www.securityfocus.com/bid/64904">http://www.securityfocus.com/bid/64904</a> url: <a href="http://www.securityfocus.com/bid/64908">http://www.securityfocus.com/bid/64908</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html">http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html</a> cert-bund: CB-K14/0710 cert-bund: CB-K14/0187 cert-bund: CB-K14/0177 cert-bund: CB-K14/0082 cert-bund: CB-K14/0074 cert-bund: CB-K14/0055 dfn-cert: DFN-CERT-2014-0742 dfn-cert: DFN-CERT-2014-0190 dfn-cert: DFN-CERT-2014-0180 dfn-cert: DFN-CERT-2014-0085 dfn-cert: DFN-CERT-2014-0074 dfn-cert: DFN-CERT-2014-0048
Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 04 (Jan 2014) - Windows
<b>Product detection result</b> 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 ...
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to InnoDB, Optimizer, Error Handling, and some unknown vectors.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2014-0401 cve: CVE-2014-0412 cve: CVE-2014-0437 cve: CVE-2013-5908 url: <a href="http://secunia.com/advisories/56491">http://secunia.com/advisories/56491</a> url: <a href="http://www.securityfocus.com/bid/64849">http://www.securityfocus.com/bid/64849</a> url: <a href="http://www.securityfocus.com/bid/64880">http://www.securityfocus.com/bid/64880</a> url: <a href="http://www.securityfocus.com/bid/64896">http://www.securityfocus.com/bid/64896</a>
...continues on next page ...

...continued from previous page ...
url: <a href="http://www.securityfocus.com/bid/64898">http://www.securityfocus.com/bid/64898</a>
url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html">http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html</a>
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 - 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

... continues on next page ...

...continued from previous page ...
Oracle MySQL version 5.5.33 and earlier on Windows, Oracle MySQL version 5.6.13 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Partition.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-5891 url: <a href="http://secunia.com/advisories/56491">http://secunia.com/advisories/56491</a> url: <a href="http://www.securityfocus.com/bid/64891">http://www.securityfocus.com/bid/64891</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html">http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html</a> cert-bund: CB-K14/0710 cert-bund: CB-K14/0187 cert-bund: CB-K14/0082 cert-bund: CB-K14/0074 cert-bund: CB-K14/0055 dfn-cert: DFN-CERT-2014-0742 dfn-cert: DFN-CERT-2014-0190 dfn-cert: DFN-CERT-2014-0085 dfn-cert: DFN-CERT-2014-0074 dfn-cert: DFN-CERT-2014-0048

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 (May 2014) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> ... continues on next page ...

...continued from previous page ...
Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.35 and earlier and 5.6.15 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Partition, Replication and XML subcomponent.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2014-0384 cve: CVE-2014-2419 cve: CVE-2014-2438 url: <a href="http://secunia.com/advisories/57940">http://secunia.com/advisories/57940</a> url: <a href="http://www.securityfocus.com/bid/66835">http://www.securityfocus.com/bid/66835</a> url: <a href="http://www.securityfocus.com/bid/66846">http://www.securityfocus.com/bid/66846</a> url: <a href="http://www.securityfocus.com/bid/66880">http://www.securityfocus.com/bid/66880</a> url: <a href="http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638">http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html">http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html</a> cert-bund: CB-K14/0710 cert-bund: CB-K14/0464
... continues on next page ...

...continued from previous page ...

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: 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.

**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: 2024-02-20T14:37:13Z

**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)
<b>References</b> cve: CVE-2013-3783 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html">http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html</a> url: <a href="http://www.securityfocus.com/bid/61210">http://www.securityfocus.com/bid/61210</a> 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 vulnerability-04 (Jul 2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier and 5.6.10 on Windows.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
Unspecified error in the MySQL Server component via unknown vectors related to Server Options.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-3808 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html">http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html</a> url: <a href="http://www.securityfocus.com/bid/61227">http://www.securityfocus.com/bid/61227</a> cert-bund: CB-K13/0620 dfn-cert: DFN-CERT-2013-1599 dfn-cert: DFN-CERT-2013-1553 dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-02 (Jul 2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote authenticated users to affect integrity and availability via unknown vectors and cause denial of service.
<b>Solution:</b> ... continues on next page ...

...continued from previous page ...
<b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL 5.5.31 and earlier, 5.6.11 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Server Replication, Audit Log and Data Manipulation Language.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-3812 cve: CVE-2013-3809 cve: CVE-2013-3793 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html">http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html</a> url: <a href="http://www.securityfocus.com/bid/61249">http://www.securityfocus.com/bid/61249</a> url: <a href="http://www.securityfocus.com/bid/61264">http://www.securityfocus.com/bid/61264</a> url: <a href="http://www.securityfocus.com/bid/61272">http://www.securityfocus.com/bid/61272</a> 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-01 (Jul 2013) - Windows
<b>Product detection result</b> 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 ...
<b>Summary</b> MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, 5.6.11 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Full Text Search and Server Optimizer.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T14:37:13Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2013-3804 cve: CVE-2013-3802 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html">http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html</a> url: <a href="http://www.securityfocus.com/bid/61244">http://www.securityfocus.com/bid/61244</a> url: <a href="http://www.securityfocus.com/bid/61260">http://www.securityfocus.com/bid/61260</a> cert-bund: CB-K13/1072 cert-bund: CB-K13/0620 dfn-cert: DFN-CERT-2013-2099
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2013-1599 dfn-cert: DFN-CERT-2013-1553 dfn-cert: DFN-CERT-2013-1478
Medium (CVSS: 4.0) NVT: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> cpe:/a:mysql:mysql:5.5.20-log Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.1.3.6.1.4.1.25623.1.0.100152)
<b>Summary</b> Oracle MySQL Server is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.30 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.30 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5 through 5.5.29.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows OID:1.3.6.1.4.1.25623.1.0.117215 Version used: 2021-02-12T11:09:59Z
<b>Product Detection Result</b> 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)
<b>References</b> ... continues on next page ...

...continued from previous page...

```

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

```

[ [return to 192.168.1.34](#) ]**2.1.19 Medium 135/tcp**

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**

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

**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:192.168.1.34[49152]

```

Port: 49153/tcp

```

  UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49153]
  Annotation: NRP server endpoint
  UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49153]
  Annotation: DHCP Client LRPC Endpoint
  UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49153]
  Annotation: DHCPv6 Client LRPC Endpoint
  UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49153]
  Annotation: Event log TCPIP

```

Port: 49154/tcp

```

  UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49154]
  UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
  Endpoint: ncacn_ip_tcp:192.168.1.34[49154]

```

...continues on next page...

...continued from previous page...	
<p>Annotation: IP Transition Configuration endpoint          UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49154]          UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49154]          Annotation: XactSrv service          UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49154]          Annotation: IKE/Authip API          UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49154]          Annotation: Impl friendly name</p>	
Port: 49155/tcp	<p>UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49155]          Named pipe : lsass          Win32 service or process : lsass.exe          Description : SAM access</p>
Port: 49204/tcp	<p>UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2          Endpoint: ncacn_ip_tcp:192.168.1.34[49204]</p>
Port: 49205/tcp	<p>UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1          Endpoint: ncacn_ip_tcp:192.168.1.34[49205]          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:192.168.1.34[49205]          Annotation: Remote Fw APIs</p>
<p>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.</p>	
<p><b>Impact</b>          An attacker may use this fact to gain more knowledge about the remote host.</p>	
<p><b>Solution:</b>  <b>Solution type:</b> Mitigation          Filter incoming traffic to this ports.</p>	
<p><b>Vulnerability Detection Method</b>          Details: DCE/RPC and MSRPC Services Enumeration Reporting          OID:1.3.6.1.4.1.25623.1.0.10736          Version used: 2022-06-03T10:17:07Z</p>	

[\[ return to 192.168.1.34 \]](#)

### 2.1.20 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<b>Product detection result</b> 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)
<b>Summary</b> This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440
... continues on next page ...



...continued from previous page ...	
Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: <a href="https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> cert-bund: CB-K21/0067 cert-bund: CB-K19/0812 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	
...continues on next page ...	

...continued from previous page ...

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  
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

...continues on next page ...

...continued from previous page ...
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
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
... continues on next page ...

...continued from previous page ...
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 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
...continues on next page ...

...continued from previous page ...	
cert-bund:	CB-K13/0790
dfn-cert:	DFN-CERT-2020-0177
dfn-cert:	DFN-CERT-2020-0111
dfn-cert:	DFN-CERT-2019-0068
dfn-cert:	DFN-CERT-2018-1441
dfn-cert:	DFN-CERT-2018-1408
dfn-cert:	DFN-CERT-2016-1372
dfn-cert:	DFN-CERT-2016-1164
dfn-cert:	DFN-CERT-2016-0388
dfn-cert:	DFN-CERT-2015-1853
dfn-cert:	DFN-CERT-2015-1332
dfn-cert:	DFN-CERT-2015-0884
dfn-cert:	DFN-CERT-2015-0800
dfn-cert:	DFN-CERT-2015-0758
dfn-cert:	DFN-CERT-2015-0567
dfn-cert:	DFN-CERT-2015-0544
dfn-cert:	DFN-CERT-2015-0530
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0375
dfn-cert:	DFN-CERT-2015-0374
dfn-cert:	DFN-CERT-2015-0305
dfn-cert:	DFN-CERT-2015-0199
dfn-cert:	DFN-CERT-2015-0079
dfn-cert:	DFN-CERT-2015-0021
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2013-1847
dfn-cert:	DFN-CERT-2013-1792
dfn-cert:	DFN-CERT-2012-1979
dfn-cert:	DFN-CERT-2012-1829
dfn-cert:	DFN-CERT-2012-1530
dfn-cert:	DFN-CERT-2012-1380
dfn-cert:	DFN-CERT-2012-1377
dfn-cert:	DFN-CERT-2012-1292
dfn-cert:	DFN-CERT-2012-1214
dfn-cert:	DFN-CERT-2012-1213
dfn-cert:	DFN-CERT-2012-1180
dfn-cert:	DFN-CERT-2012-1156
dfn-cert:	DFN-CERT-2012-1155
dfn-cert:	DFN-CERT-2012-1039
dfn-cert:	DFN-CERT-2012-0956
dfn-cert:	DFN-CERT-2012-0908
dfn-cert:	DFN-CERT-2012-0868
dfn-cert:	DFN-CERT-2012-0867
dfn-cert:	DFN-CERT-2012-0848
dfn-cert:	DFN-CERT-2012-0838
dfn-cert:	DFN-CERT-2012-0776
dfn-cert:	DFN-CERT-2012-0722
...continues on next page ...	

...continued from previous page ...

```

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%****Vulnerability Detection Result**

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

Subject: CN=vagrant-2008R2

Signature Algorithm: sha1WithRSAEncryption

...continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

[\[ return to 192.168.1.34 \]](#)

### 2.1.21 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
<b>Product detection result</b> cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ... continues on next page ...

...continued from previous page ...	
↔)	
<b>Summary</b> The remote SSH server is configured to allow / support weak MAC algorithm(s).	
<b>Quality of Detection (QoD): 80%</b>	
<b>Vulnerability Detection Result</b> 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	
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak MAC algorithm(s).	
<b>Vulnerability Detection Method</b> 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	
<b>Product Detection Result</b> Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)	
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc6668">https://www.rfc-editor.org/rfc/rfc6668</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.4">https://www.rfc-editor.org/rfc/rfc4253#section-6.4</a>	

[ [return to 192.168.1.34](#) ]



**2.1.22 Low general/tcp**

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 304898 Packet 2: 305040
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...
url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a>
url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>
url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[\[ return to 192.168.1.34 \]](#)

### 2.1.23 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: <ul style="list-style-type: none"> <li>- ICMP Type: 14</li> <li>- ICMP Code: 0</li> </ul>
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: <ul style="list-style-type: none"> <li>- Disable the support for ICMP timestamp on the remote host completely</li> <li>- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)</li> </ul>
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190
... continues on next page ...

...continued from previous page ...
Version used: 2023-05-11T09:09:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.1.34 \]](#)

### 2.1.24 Low 9200/tcp

Low (CVSS: 3.1)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)
<b>Summary</b> Elasticsearch is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 1.1.1 Fixed version: 6.8.13 Installation path / port: /
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.8.13, 7.9.2 or later.
<b>Affected Software/OS</b> Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.
<b>Vulnerability Insight</b>
... continues on next page ...

...continued from previous page ...
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.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13) OID:1.3.6.1.4.1.25623.1.0.117181 Version used: 2021-08-17T12:00:57Z
<b>References</b> cve: CVE-2020-7020 url: <a href="https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update/253033">https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update/253033</a> url: <a href="https://www.elastic.co/community/security">https://www.elastic.co/community/security</a> cert-bund: WID-SEC-2022-0607 dfn-cert: DFN-CERT-2022-1530

[\[ return to 192.168.1.34 \]](#)

### 2.1.25 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
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.
<b>Vulnerability Insight</b> An unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Connection' sub-component.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (. ↔.. OID:1.3.6.1.4.1.25623.1.0.808593 Version used: 2022-04-13T13:17:10Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-5444 url: <a href="https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/91987">http://www.securityfocus.com/bid/91987</a> advisory-id: cpujul2016 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)

... continues on next page ...

...continued from previous page...	
<b>Summary</b>	Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b>	80%
<b>Vulnerability Detection Result</b>	Installed version: 5.5.20 Fixed version: See the referenced vendor advisory Installation path / port: 3306/tcp
<b>Impact</b>	Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.
<b>Solution:</b>	<b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b>	Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.10.
<b>Vulnerability Insight</b>	An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Security Encryption' sub-component.
<b>Vulnerability Detection Method</b>	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: 2022-04-13T13:17:10Z
<b>Product Detection Result</b>	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)
<b>References</b>	cve: CVE-2016-3452 url: <a href="https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL</a> url: <a href="http://www.securityfocus.com/bid/91999">http://www.securityfocus.com/bid/91999</a> advisory-id: cpujul2016 dfn-cert: DFN-CERT-2016-1192 dfn-cert: DFN-CERT-2016-1169

Low (CVSS: 3.5)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 (Oct 2015) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:      Apply the patch Installation path / port:        3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to affect integrity via unknown vectors.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on windows
<b>Vulnerability Insight</b> Unspecified error exists in the MySQL Server component via unknown vectors related to Server.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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 ...
<b>References</b> cve: CVE-2015-4864 url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html">http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html</a> url: <a href="http://www.securityfocus.com/bid/77187">http://www.securityfocus.com/bid/77187</a> cert-bund: WID-SEC-2024-1483 cert-bund: CB-K15/1844 cert-bund: CB-K15/1554 dfn-cert: DFN-CERT-2016-0265 dfn-cert: DFN-CERT-2015-1946 dfn-cert: DFN-CERT-2015-1638

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-04 (Jul 2015)
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version:       Apply the patch Installation path / port:       3306/tcp
<b>Impact</b> Successful exploitation will allow an authenticated remote attacker to cause denial of service attack.
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on Windows.
<b>Vulnerability Insight</b> ... continues on next page ...



...continued from previous page ...
Unspecified error exists in the MySQL Server component via unknown vectors related to Server : Optimizer.
<b>Vulnerability Detection Method</b> 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: 2024-02-20T05:05:48Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2015-4757 url: <a href="http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html">http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html</a> url: <a href="http://www.securityfocus.com/bid/75759">http://www.securityfocus.com/bid/75759</a> 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 Server Multiple Vulnerabilities - 05 - (Nov 2012) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20
... continues on next page ...

...continued from previous page ...	
Fixed version:	Apply the patch
<b>Impact</b> Successful exploitation will allow an attacker to disclose potentially sensitive information and manipulate certain data.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the linked references or upgrade to latest version.	
<b>Affected Software/OS</b> Oracle MySQL version 5.5.x to 5.5.25 on Windows.	
<b>Vulnerability Insight</b> The flaw is due to unspecified error in MySQL server component vectors server.	
<b>Vulnerability Detection Method</b> Details: Oracle MySQL Server Multiple Vulnerabilities - 05 - (Nov 2012) - Windows OID:1.3.6.1.4.1.25623.1.0.803115 Version used: 2024-02-09T05:06:25Z	
<b>Product Detection Result</b> 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)	
<b>References</b> cve: CVE-2012-3156 url: <a href="http://secunia.com/advisories/51008/">http://secunia.com/advisories/51008/</a> url: <a href="http://www.securityfocus.com/bid/56013">http://www.securityfocus.com/bid/56013</a> url: <a href="http://www.securelist.com/en/advisories/51008">http://www.securelist.com/en/advisories/51008</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html">http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html</a> url: <a href="https://support.oracle.com/rs?type=doc&amp;id=1475188.1">https://support.oracle.com/rs?type=doc&amp;id=1475188.1</a>	
Low (CVSS: 2.8)	
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 (Jan 2014) - Windows	
<b>Product detection result</b> 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 ...
<b>Summary</b> Oracle MySQL is prone to multiple unspecified vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).
<b>Solution:</b> <b>Solution type:</b> VendorFix Apply the patch from the referenced advisory.
<b>Affected Software/OS</b> Oracle MySQL version 5.5.34 and earlier, and 5.6.14 and earlier on Windows.
<b>Vulnerability Insight</b> Unspecified errors in the MySQL Server component via unknown vectors related to Replication.
<b>Vulnerability Detection Method</b> 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: 2024-02-09T05:06:25Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2014-0420 url: <a href="http://secunia.com/advisories/56491">http://secunia.com/advisories/56491</a> url: <a href="http://www.securityfocus.com/bid/64888">http://www.securityfocus.com/bid/64888</a> url: <a href="http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html">http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html</a> 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
... continues on next page ...

dfn-cert: DFN-CERT-2014-0085 dfn-cert: DFN-CERT-2014-0074 dfn-cert: DFN-CERT-2014-0048
--

...continued from previous page ...

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.6.45 Installation path / port: 3306/tcp
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.6.45, 5.7.19 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.6.44 and prior and 5.7 through 5.7.18.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Wi. ↵.. OID:1.3.6.1.4.1.25623.1.0.142643 Version used: 2021-09-07T14:01:38Z
<b>Product Detection Result</b> 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-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: 2.7)

NVT: Oracle MySQL Server &lt;= 5.7.40, 8.x &lt;= 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

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 &lt;= 5.7.40, 8.x &lt;= 8.0.31 Security Update (cpuapr2023) - Win.↵..

OID:1.3.6.1.4.1.25623.1.0.149532

Version used: 2023-10-13T05:06:10Z

**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)
<b>References</b> cve: CVE-2023-21963 url: <a href="https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL">https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL</a> advisory-id: cpuapr2023 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1033 dfn-cert: DFN-CERT-2023-0885

Low (CVSS: 1.5)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) - Windows
<b>Product detection result</b> 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)
<b>Summary</b> Oracle MySQL Server is prone to an unspecified vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 5.5.20 Fixed version: 5.5.31 Installation path / port: 3306/tcp
<b>Impact</b> Successful exploitation will allow local users to affect availability.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.5.31, 5.6.10 or later.
<b>Affected Software/OS</b> Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.9.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
An unspecified error exists in the MySQL Server component via unknown vectors related to Server Partition.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) -. ↔.. OID:1.3.6.1.4.1.25623.1.0.809813 Version used: 2022-04-25T14:50:49Z
<b>Product Detection Result</b> 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)
<b>References</b> 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 192.168.1.34](#) ]