# Scan Report

January 27, 2023

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 172.16.1.8". The scan started at Fri Jan 13 12:34:41 2023 UTC and ended at Fri Jan 13 16:09:10 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 172.16.1.8 | 68 | 136 | 12 | 0 | 0 |
| Total: 1 | 68 | 136 | 12 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 216 results selected by the filtering described above. Before filtering there were 387 results.

# 2 Results per Host

## 2.1 172.16.1.8

| | |
|---|---|
| Host scan start | Fri Jan 13 12:35:41 2023 UTC |
| Host scan end | Fri Jan 13 16:09:06 2023 UTC |

| Service (Port) | Threat Level |
|---|---|
| 4848/tcp | High |
| 8022/tcp | High |
| 8020/tcp | High |
| 3000/tcp | High |
| 445/tcp | High |
| 22/tcp | High |
| 9200/tcp | High |
| 8019/tcp | High |
| 8009/tcp | High |
| 8383/tcp | High |
| 8282/tcp | High |
| 3306/tcp | High |
| 4848/tcp | Medium |
| 135/tcp | Medium |
| 8022/tcp | Medium |
| 8020/tcp | Medium |

. . . (continues) . . .

... (continued) ...

| Service (Port) | Threat Level |
|---|---|
| 3000/tcp | Medium |
| 22/tcp | Medium |
| 9200/tcp | Medium |
| 8181/tcp | Medium |
| 3389/tcp | Medium |
| 8383/tcp | Medium |
| 8282/tcp | Medium |
| 3306/tcp | Medium |
| 8443/tcp | Medium |
| general/icmp | Low |
| 9200/tcp | Low |
| general/tcp | Low |
| 3306/tcp | Low |

### 2.1.1 High 4848/tcp

High (CVSS: 7.5)
NVT: Oracle Glass Fish Server Directory Traversal Vulnerability

**Summary**
Glass fish server is prone to a directory traversal vulnerability.

**Vulnerability Detection Result**
`Vulnerable URL: https://172.16.1.8:4848/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/%c0%ae%c0%ae/windows/win.ini`

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

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

**Affected Software/OS**
Oracle Glassfish Server version 4.1.1 and probably prior.

**Vulnerability Insight**
The flaw is due to
- Improper sanitization of parameter 'META-INF' in 'theme.php' file.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Send a crafted request via HTTP GET and check whether it is able to get the content of passwd file.
Details: Oracle Glass Fish Server Directory Traversal Vulnerability
OID:1.3.6.1.4.1.25623.1.0.806848
Version used: 2021-10-11T08:01:31Z

**References**
cve: CVE-2017-1000028
url: https://www.exploit-db.com/exploits/39241

[ return to 172.16.1.8 ]

### 2.1.2 High 8022/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

**Summary**
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

**Vulnerability Detection Result**
Installed version: 9.1.084
Fixed version: 10.0.082
Installation
path / port: /

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.082 or later.

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.082.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.
↪..
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-

... continues on next page ...

... continued from previous page ...

↪control-privilege-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

**Summary**
ManageEngine Desktop Central is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
Installed version: 9.1.084
Fixed version: 10.0.157
Installation
path / port: /

**Impact**
Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.157 or later.

**Affected Software/OS**
ManageEngine Desktop Central/MSP version 10.0.137 and prior.

**Vulnerability Insight**
This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure .
↪..
OID:1.3.6.1.4.1.25623.1.0.812522
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2017-16924
url: https://vuldb.com/?id.113555
url: https://www.manageengine.com/desktop-management-msp/password-encryption-pol
↪icy-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`Vulnerable URL: http://172.16.1.8:8022/jsp/admin/DBQueryExecutor.jsp?actionFrom=`
`↪getResult&query=SELECT%20*%20from%20aaauser;`

**Impact**
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.208 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 10.0.184 and prior.

**Vulnerability Insight**
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

**References**
`cve: CVE-2018-5337`
`cve: CVE-2018-5338`
`cve: CVE-2018-5339`
`cve: CVE-2018-5341`
`url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln`
`↪erabilities-in-manageengine-desktop-central`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

**Summary**

. . . continues on next page . . .

... continued from previous page ...

ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

**Vulnerability Detection Result**

```
It was possible to upload the file 'http://172.16.1.8:8022/jspf/GBNVT_CVE-2015-8
↪249_test.jsp'. Please delete this file.
```

**Impact**

Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

**Solution:**

**Solution type:** VendorFix

Update to version 9.0.142 or later.

**Affected Software/OS**

ManageEngine Desktop Central prior to version 9.0.142.

**Vulnerability Detection Method**

Try to upload a jsp file.

Details: `ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi.
↪..`

OID:1.3.6.1.4.1.25623.1.0.140041

Version used: `2021-10-12T12:01:25Z`

**References**

`cve: CVE-2015-8249`

## High (CVSS: 9.8)

## NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

**Summary**

ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

**Vulnerability Detection Result**

```
Installed version: 9.1.084
Fixed version:     10.0.092
Installation
path / port:       /
```

**Solution:**

**Solution type:** VendorFix

Update to version 10.0.092 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.092.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.092 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: `2021-09-23T03:58:52Z`

**References**
`cve: CVE-2017-11346`
`url: https://www.manageengine.com/products/desktop-central/remote-code-execution.html`

[ return to 172.16.1.8 ]

### 2.1.3 High 8020/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

**Summary**
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     10.0.082
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.082 or later.

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.082.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln..`
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: `2021-09-23T03:58:52Z`

... continues on next page ...

... continued from previous page ...

**References**
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-control-privilege-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Vulnerable URL: http://172.16.1.8:8020/jsp/admin/DBQueryExecutor.jsp?actionFrom=getResult&query=SELECT%20*%20from%20aaauser;

**Impact**
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.208 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 10.0.184 and prior.

**Vulnerability Insight**
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2018-5337
cve: CVE-2018-5338
cve: CVE-2018-5339
cve: CVE-2018-5341

... continues on next page ...

... continued from previous page ...

url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln
↪erabilities-in-manageengine-desktop-central

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

**Summary**
ManageEngine Desktop Central is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
Installed version: 9.1.084
Fixed version: 10.0.157
Installation
path / port: /

**Impact**
Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.157 or later.

**Affected Software/OS**
ManageEngine Desktop Central/MSP version 10.0.137 and prior.

**Vulnerability Insight**
This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure .
↪..
OID:1.3.6.1.4.1.25623.1.0.812522
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2017-16924
url: https://vuldb.com/?id.113555
url: https://www.manageengine.com/desktop-management-msp/password-encryption-pol
↪icy-violation.html

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability

**Summary**
ManageEngine Desktop Central is prone to an arbitrary file upload vulnerability.

**Vulnerability Detection Result**
`It was possible to upload the file "/gbnvt1763331721.jsp". Please delete this fi`
`↪le.`
`Vulnerable URL: http://172.16.1.8:8020/agentLogUploader?computerName=DesktopCent`
`↪ral&domainName=webapps&customerId=1&filename=gbnvt1763331721.jsp`

**Impact**
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

**Solution:**
**Solution type:** VendorFix
Update to version 8.0.293 or later.

**Affected Software/OS**
ManageEngine Desktop Central prior to version 8.0.293.

**Vulnerability Insight**
The flaw in the AgentLogUploadServlet. This servlet takes input from HTTP POST and constructs an output file on the server without performing any sanitisation or even checking if the caller is authenticated.

**Vulnerability Detection Method**
Sends a crafted HTTP POST request and checks the response.
Details: `ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.803777
Version used: `2021-10-15T09:03:25Z`

**References**
`cve: CVE-2013-7390`
`cve: CVE-2014-5007`
`url: http://www.exploit-db.com/exploits/29674`
`url: http://security-assessment.com/files/documents/advisory/DesktopCentral%20Ar`
`↪bitrary%20File%20Upload.pdf`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

**Summary**
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Result**
`It was possible to upload the file 'http://172.16.1.8:8020/jspf/GBNVT_CVE-2015-8249_test.jsp'. Please delete this file.`

**Impact**
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

**Solution:**
**Solution type:** VendorFix
Update to version 9.0.142 or later.

**Affected Software/OS**
ManageEngine Desktop Central prior to version 9.0.142.

**Vulnerability Detection Method**
Try to upload a jsp file.
Details: `ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi..`
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: `2021-10-12T12:01:25Z`

**References**
`cve: CVE-2015-8249`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

**Summary**
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     10.0.092
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.092 or later.

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.092.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2017-11346
url: https://www.manageengine.com/products/desktop-central/remote-code-execution
↪.html

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

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

**Vulnerability Detection Result**
Vulnerable URL: http://172.16.1.8:8020/.//WEB-INF/web.xml
Response (truncated):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
```

... continues on next page ...

... continued from previous page ...

```
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

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

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

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

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: '/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: 2021-10-11T08:01:31Z

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

[ return to 172.16.1.8 ]

### 2.1.4 High 3000/tcp

High (CVSS: 9.8)
NVT: Ruby on Raily < 5.2.4.3, 6.x < 6.0.3.1 Multiple Vulnerabilities (Windows)

**Summary**
Ruby on Rails is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 4.1.1
Fixed version: 5.2.4.3
Installation
path / port: /

**Solution:**
**Solution type:** VendorFix
Update to version 5.2.4.3 or 6.0.3.1 respectively.

**Affected Software/OS**
Ruby on Rails through version 5.2.4.2 and versions 6.0.0.0 through 6.0.3.0.

**Vulnerability Insight**
The following vulnerabilities exist:
- The Content-Length parameter of a direct file upload may be modified by an attacker to bypass upload limitations.
- A deserialization vulnerability may allow an attacker to read sensitive information.
- An attacker may unmarshal user-provided objects in MemCacheStore and RedisCacheStore resulting in arbitrary code execution.

... continues on next page ...

... continued from previous page ...

- A cross-site request forgery (CSRF) vulnerability in the rails-ujs module may allow an attacker to perform actions in the context of another user.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Raily < 5.2.4.3, 6.x < 6.0.3.1 Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.113712
Version used: `2021-07-07T11:00:41Z`

**References**
`cve: CVE-2020-8162`
`cve: CVE-2020-8164`
`cve: CVE-2020-8165`
`cve: CVE-2020-8167`
`url: https://weblog.rubyonrails.org/2020/5/18/Rails-5-2-4-3-and-6-0-3-1-have-bee`
`↪n-released/`
`url: https://hackerone.com/reports/789579`
`url: https://hackerone.com/reports/292797`
`url: https://hackerone.com/reports/413388`
`url: https://hackerone.com/reports/189878`
`cert-bund: CB-K20/0477`
`dfn-cert: DFN-CERT-2021-0842`
`dfn-cert: DFN-CERT-2020-2327`
`dfn-cert: DFN-CERT-2020-2240`
`dfn-cert: DFN-CERT-2020-2093`
`dfn-cert: DFN-CERT-2020-2058`
`dfn-cert: DFN-CERT-2020-1582`
`dfn-cert: DFN-CERT-2020-1323`

High (CVSS: 8.8)
NVT: Ruby on Rails < 5.0.1 RCE Vulnerability

**Summary**
Ruby on Rails is prone to a remote code execution (RCE) vulnerability.

**Vulnerability Detection Result**
`Installed version: 4.1.1`
`Fixed version: 5.0.1`
`Installation`
`path / port: /`

**Impact**
Successful exploitation would allow an attacker to execute arbitrary code on the target machine.

**Solution:**
**Solution type:** VendorFix
Update to version 5.0.1 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Ruby on Rails through version 5.0.0.

**Vulnerability Insight**
An attacker may exploit this vulnerability by sending a specially crafted 'render' call.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails < 5.0.1 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113718
Version used: `2021-07-07T11:00:41Z`

**References**
`cve: CVE-2020-8163`
`url: https://hackerone.com/reports/304805`
`cert-bund: CB-K20/0472`
`dfn-cert: DFN-CERT-2020-1733`
`dfn-cert: DFN-CERT-2020-1582`

High (CVSS: 7.5)
NVT: Ruby on Rails Multiple Vulnerabilities-01 Oct16 (Windows)

**Summary**
Ruby on Rails is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 4.1.1
Fixed version:     4.1.14.1
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow a remote attacker to read arbitrary files by leveraging an application's unrestricted use of the render method, to cause a denial of service.

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 3.2.22.1 or 4.1.14.1 or 4.2.5.1, or later.

**Affected Software/OS**
Ruby on Rails before 3.2.22.1, Ruby on Rails 4.0.x and 4.1.x before 4.1.14.1 and Ruby on Rails 4.2.x before 4.2.5.1 on Windows.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
Multiple flaws are due to:
- Directory traversal vulnerability in Action View.
- The script 'actionpack/lib/action_dispatch/http/mime_type.rb' does not properly restrict use of the MIME type cache.
- The http_basic_authenticate_with method in 'actionpack/lib/action_controller/metal/http_authentication.rb' does not use a constant-time algorithm for verifying credentials.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Multiple Vulnerabilities-01 Oct16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809356
Version used: `2022-08-09T10:11:17Z`

**References**
`cve: CVE-2016-0752`
`cve: CVE-2016-0751`
`cve: CVE-2015-7576`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: http://www.openwall.com/lists/oss-security/2016/01/25/10`
`url: http://www.securityfocus.com/bid/81801`
`url: http://www.securityfocus.com/bid/81800`
`url: http://www.securityfocus.com/bid/81803`
`cert-bund: CB-K17/0517`
`cert-bund: CB-K17/0278`
`cert-bund: CB-K16/0625`
`cert-bund: CB-K16/0522`
`cert-bund: CB-K16/0419`
`cert-bund: CB-K16/0238`
`cert-bund: CB-K16/0166`
`cert-bund: CB-K16/0165`
`dfn-cert: DFN-CERT-2017-0534`
`dfn-cert: DFN-CERT-2017-0284`
`dfn-cert: DFN-CERT-2016-0674`
`dfn-cert: DFN-CERT-2016-0566`
`dfn-cert: DFN-CERT-2016-0458`
`dfn-cert: DFN-CERT-2016-0259`
`dfn-cert: DFN-CERT-2016-0181`
`dfn-cert: DFN-CERT-2016-0178`

High (CVSS: 7.5)
NVT: Ruby on Rails Action Pack Denial of Service Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 4.1.1
Fixed version: 4.2.5.1
Installation
path / port: /

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

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

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

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

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Action Pack Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.809362
Version used: 2022-04-13T13:17:10Z

**References**
cve: CVE-2015-7581
url: http://www.openwall.com/lists/oss-security/2016/01/25/14
url: http://www.securityfocus.com/bid/81677
cert-bund: CB-K16/0625
cert-bund: CB-K16/0419
cert-bund: CB-K16/0166
cert-bund: CB-K16/0165
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2016-0178

## High (CVSS: 7.3)
## NVT: Ruby on Rails Action Pack Remote Code Execution Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a remote code execution (RCE) vulnerability.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
Installed version: 4.1.1
Fixed version:     4.1.14.2
Installation
path / port:       /
```

**Impact**

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

**Solution:**

**Solution type:** VendorFix

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

**Affected Software/OS**

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

**Vulnerability Insight**

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

**Vulnerability Detection Method**

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

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

OID:1.3.6.1.4.1.25623.1.0.809352

Version used: `2022-04-13T13:17:10Z`

**References**

```
cve: CVE-2016-2098
url: https://www.debian.org/security/2016/dsa-3509
url: http://www.securityfocus.com/bid/83725
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/ly-IH-
↪fxr_Q/WLoOhcMZIAAJ
cert-bund: WID-SEC-2022-2271
cert-bund: CB-K17/1730
cert-bund: CB-K16/0625
cert-bund: CB-K16/0522
cert-bund: CB-K16/0426
cert-bund: CB-K16/0419
cert-bund: CB-K16/0372
dfn-cert: DFN-CERT-2017-1809
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0566
dfn-cert: DFN-CERT-2016-0468
dfn-cert: DFN-CERT-2016-0458
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0404

[ return to 172.16.1.8 ]

### 2.1.5 High 445/tcp

High (CVSS: 8.1)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

**Summary**
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

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

**Impact**
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

**Solution:**
**Solution type:** VendorFix
The vendor has released updates. Please see the references for more information.

**Affected Software/OS**
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

**Vulnerability Insight**
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

**Vulnerability Detection Method**
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2022-08-09T10:11:17Z`

... continues on next page ...

... continued from previous page ...

**References**

cve: CVE-2017-0143
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448

[ return to 172.16.1.8 ]

### 2.1.6 High 22/tcp

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

**Product detection result**

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

**Summary**

openssh is prone to a security bypass vulnerability.

**Vulnerability Detection Result**

Installed version: 7.1
Fixed version: 7.2
Installation
path / port: 22/tcp

**Impact**

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

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** VendorFix
Upgrade to OpenSSH version 7.2 or later.

**Affected Software/OS**
OpenSSH versions before 7.2 on Windows

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

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.810768
Version used: `2022-08-22T10:11:10Z`

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

**References**
`cve: CVE-2016-1908`
`url: http://openwall.com/lists/oss-security/2016/01/15/13`
`url: http://www.securityfocus.com/bid/84427`
`url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4`
`url: http://www.openssh.com/txt/release-7.2`
`url: https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0`
`↪db113c71e234416c`
`url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741`
`cert-bund: CB-K16/1485`
`cert-bund: CB-K16/0694`
`cert-bund: CB-K16/0684`
`cert-bund: CB-K16/0449`
`cert-bund: CB-K16/0162`
`dfn-cert: DFN-CERT-2018-1828`
`dfn-cert: DFN-CERT-2016-1574`
`dfn-cert: DFN-CERT-2016-0754`
`dfn-cert: DFN-CERT-2016-0733`
`dfn-cert: DFN-CERT-2016-0488`
`dfn-cert: DFN-CERT-2016-0182`

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

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

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

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

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

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

**Vulnerability Detection Method**
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2022-08-04T13:37:02Z`

**References**
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`

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.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 7.1
Fixed version: 7.3
Installation
path / port: 22/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to OpenSSH version 7.3 or later.

**Affected Software/OS**
OpenSSH versions before 7.3 on Windows

**Vulnerability Insight**
Multiple flaws exist due to:
- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.
- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

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

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

**References**
cve: CVE-2016-6515
cve: CVE-2016-6210
url: http://www.openssh.com/txt/release-7.3
url: http://www.securityfocus.com/bid/92212
url: http://seclists.org/fulldisclosure/2016/Jul/51
url: https://security-tracker.debian.org/tracker/CVE-2016-6210

... continues on next page ...

... continued from previous page ...

```
url: http://openwall.com/lists/oss-security/2016/08/01/2
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1753
cert-bund: CB-K17/1349
cert-bund: CB-K17/1292
cert-bund: CB-K17/0055
cert-bund: CB-K16/1837
cert-bund: CB-K16/1629
cert-bund: CB-K16/1487
cert-bund: CB-K16/1485
cert-bund: CB-K16/1252
cert-bund: CB-K16/1221
cert-bund: CB-K16/1082
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1407
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1729
dfn-cert: DFN-CERT-2016-1576
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-1331
dfn-cert: DFN-CERT-2016-1243
dfn-cert: DFN-CERT-2016-1149
```

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

**Product detection result**

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

**Summary**

openssh is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 7.1
Fixed version:     7.4
```

... continues on next page ...

... continued from previous page ...

Installation
path / port: 22/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to OpenSSH version 7.4 or later.

**Affected Software/OS**
OpenSSH versions before 7.4 on Windows.

**Vulnerability Insight**
Multiple flaws exist due to:
- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.
- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.
- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.
- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

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

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

**References**
cve: CVE-2016-10009
cve: CVE-2016-10010
cve: CVE-2016-10011
cve: CVE-2016-10012
cve: CVE-2016-10708
url: https://www.openssh.com/txt/release-7.4
url: http://www.securityfocus.com/bid/94968
url: http://www.securityfocus.com/bid/94972

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/94977
url: http://www.securityfocus.com/bid/94975
url: http://www.openwall.com/lists/oss-security/2016/12/19/2
url: http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
url: https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93
↪3e6b931de1d16737
cert-bund: CB-K18/0919
cert-bund: CB-K18/0591
cert-bund: CB-K18/0137
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1292
cert-bund: CB-K17/1061
cert-bund: CB-K17/0527
cert-bund: CB-K17/0377
cert-bund: CB-K17/0127
cert-bund: CB-K17/0041
cert-bund: CB-K16/1991
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-1432
dfn-cert: DFN-CERT-2018-1112
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-1068
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-1096
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0386
dfn-cert: DFN-CERT-2017-0130
dfn-cert: DFN-CERT-2017-0042
dfn-cert: DFN-CERT-2016-2099
```

[ return to 172.16.1.8 ]

### 2.1.7 High 9200/tcp

High (CVSS: 10.0)
NVT: Elasticsearch End of Life (EOL) Detection

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

**Vulnerability Detection Result**
```
The "Elasticsearch" version on the remote host has reached the end of life.
CPE:               cpe:/a:elastic:elasticsearch:1.1.1
Installed version: 1.1.1
EOL version:       1.1
EOL date:          2015-09-25
```

**Impact**
An EOL version of Elasticsearch is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution:**
**Solution type:** VendorFix
Update Elasticsearch to a version that still receives technical support and updates.

**Vulnerability Detection Method**
Checks if an EOL version is present on the target host.
Details: `Elasticsearch End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.113131
Version used: `2021-01-18T10:09:47Z`

**References**
`url: https://www.elastic.co/support/eol`

High (CVSS: 9.8)
NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)

**Summary**
Elasticsearch is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 1.1.1
Fixed version:     1.6.1
```

**Impact**
Successful exploitation will allow remote attackers to execute code or read arbitrary files.

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

. . . continues on next page . . .

... continued from previous page ...

Update to Elasticsearch version 1.6.1, or later.

**Affected Software/OS**
Elasticsearch version 1.0.0 through 1.6.0 on Windows.

**Vulnerability Insight**
The Flaw is due to:
- an error in the snapshot API calls (CVE-2015-5531)
- an attack that can result in remote code execution (CVE-2015-5377).

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808091
Version used: `2022-04-13T13:17:10Z`

**References**
`cve: CVE-2015-5531`
`cve: CVE-2015-5377`
`url: https://www.elastic.co/community/security/`
`url: http://www.securityfocus.com/bid/75935`
`url: http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded`
`cert-bund: CB-K15/1118`
`dfn-cert: DFN-CERT-2015-1160`

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

**Summary**
Elasticsearch is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
`Installed version: 1.1.1`
`Fixed version: 5.6.12`

**Impact**
Successful exploitation would allow an authenticated attacker to acquire valid login credentials.

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.12 or 6.4.1 respectively.

**Affected Software/OS**
Elasticsearch versions through 5.6.11 and 6.0.0 through 6.4.0.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The _cluster/settings API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability (Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.113276
Version used: 2021-05-28T04:00:18Z

**References**
cve: CVE-2018-3831
url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update
↪/149035
url: https://www.elastic.co/community/security
dfn-cert: DFN-CERT-2020-1653

[ return to 172.16.1.8 ]

### 2.1.8 High 8019/tcp

High (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

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

**Vulnerability Detection Result**
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB Â¶\x0004 Ã\x0088 \x0002OK \x0005
Accept-Ranges \x0005bytes \x0004ETag \x0018W/"490059-1444224756000"
Last-Modified \x001DWed, 07 Oct 2015 13:32:36 GMT \x000CContent-Type \x0016te
↪xt/xml;charset=UTF-8 \x000EContent-Length \x0006490059 AB\x001FÃ¼\x0003\x001
↪FÃ¸<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>

... continues on next page ...

... continued from previous page ...

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

 <filter>
         <filter-name>Security_Filter</filter-name>
         <filter-class>com.adventnet.iam.security.SecurityFilter</filter-class>
         <init-param>
             <param-name>config-file</param-name>
             <param-value>security-properties.xml,security-common.xml,security.x
↪ml</param-value>
         </init-param>
         <init-param>
             <param-name>development.mode</param-name>
```

... continues on next page ...

... continued from previous page ...

```
            <param-value>false</param-value>
        </init-param>
        <init-param>
            <param-name>exclude</param-name>
            <param-value>/.*</param-value>
        </init-param>
    </filter>
    <filter-mapping>
        <filter-name>Security_Filter</filter-name>
        <url-pattern>/.*</url-pattern>
    </filter-mapping>

  <filter>
        <filter-name>DCXSSFilter</filter-name>
  <filter-class>com.adventnet.sym.webclient.xss.DCXSSFilter</filter-class>
↪

        <init-param>
            <param-name>exclude</param-name>
            <param-value>/.*\.js|/.*\.css|/.*\.txt|/.*\.html|/.*\.ico|/.*\.gif|
↪/.*\.jpg|/.*\.png|/.*\.xml</param-value>
        </init-param>
    </filter>
    <filter-mapping>
        <filter-name>DCXSSFilter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>

 <!-- Added for RAD Development -->
 <filter>
 <filter-name>StateFilter</filter-name>
 <filter-class>com.adventnet.client.view.web.StateFilter</filter-class>
 </filter>
 <filter-mapping>
 <filter-name>StateFilter</filter-name>
 <url-pattern>/STATE_ID/*</url-pattern>
 </filter-mapping>
 <!-- Ended for RAD Development -->
 <filter>
 <filter-name>URLRedirectionFilter</filter-name>
 <filter-class>com.adventnet.sym.webclient.filter.URLRedirectionFilter</filter-
↪class>
 </filter>
 <filter-mapping>
 <filter-name>URLRedirectionFilter</filter-name>
 <url-pattern>/client-data/*</url-pattern>
 </filter-mapping>
```

... continues on next page ...

... continued from previous page ...

```
 <filter-mapping>
 <filter-name>URLRedirectionFilter</filter-name>
 <url-pattern>/agent/*</url-pattern>
 </filter-mapping>
 <!-- MSP Specific Filter-->
 <filter>
 <filter-name>MSPCustomerFilter</filter-name>
 <filter-class>com.me.devicemanagement.framework.webclient.filter.MSPCustomerFi
↪lter</filter-class>
 </filter>
 <filter-mapping>
 <filter-name>MSPCustomerFilter</filter-name>
 <url-pattern>/*</url-pattern>
 <dispatcher>FORWARD</dispatcher>
 <dispatcher>REQUEST</dispatcher>
 </filter-mapping>

 <filter>
 <filter-name>UIRestrictionFilter</filter-name>
 <filter-class>com.adventnet.sym.webclient.filter.UIRestrictionFilter</filter-c
↪lass>
 </filter>
 <filter-mapping>
 <filter-name>UIRestrictionFilter</filter-name>
 <url-pattern>*.do</url-pattern>
 <dispatcher>FORWARD</dispatcher>
 <dispatcher>REQUEST</dispatcher>
 <dispatcher>INCLUDE</dispatcher>
 <dispatcher>ERROR</dispatcher>
 </filter-mapping>
 <filter>
 <filter-name>DCAuthorizationFilter</filter-name>
 <filter-class>com.adventnet.sym.webclient.filter.DCAuthorizationFilter</filter
↪-class>
 </filter>
 <filter-mapping>
 <filter-name>DCAuthorizationFilter</filter-name>
 <url-pattern>*.do</url-pattern>
 </filter-mapping>
        <filter>
 <filter-name>LicenseFilter</filter-name>
 <filter-class>com.me.devicemanagement.framework.webclient.filter.LicenseFilter
↪</filter-class>
 </filter>

 <filter-mapping>
 <filter-name>LicenseFilter</filter-name>
```

... continues on next page ...

... continued from previous page ...

```
 <url-pattern>/mdmTab.do</url-pattern>
 <url-pattern>/mdmAgentSettings.do</url-pattern>
 <url-pattern>/mdmLocation.do</url-pattern>
 <url-pattern>/mdmEnroll.do</url-pattern>
 <url-pattern>/mdmCustomDeviceDetails.do</url-pattern>
 <url-pattern>/mdmapns.do</url-pattern>
 <url-pattern>/mdmWPAppRepSettings.do</url-pattern>
 <url-pattern>/mdmWPAET.do</url-pattern>
 <url-pattern>/mdmEnrollSettings.do</url-pattern>
 <url-pattern>/mdmAppleConfig.do</url-pattern>
 <url-pattern>/mdmAuthentication.do</url-pattern>
 <url-pattern>/mdmBulkEnroll.do</url-pattern>
 <url-pattern>/mdmInv.do</url-pattern>
 <url-pattern>/mdmApp.do</url-pattern>
 <url-pattern>/mdmDeviceDetails.do</url-pattern>
 <url-pattern>/mdmInvDeviceScan.do</url-pattern>
 <url-pattern>/adminEmail.do</url-pattern>
 <url-pattern>/mdmReports.do</url-pattern>
 <url-pattern>/deviceMgmt.do</url-pattern>
 <url-pattern>/vppMgmt.do</url-pattern>
 <url-pattern>/appMgmt.do</url-pattern>
 <url-pattern>/appMgmtSource.do</url-pattern>
 <url-pattern>/addMoreLicense.do</url-pattern>
 <url-pattern>/appMgmtCatalogue.do</url-pattern>
 <url-pattern>/profileAudit.do</url-pattern>
 <url-pattern>/profileMgmt.do</url-pattern>
 <url-pattern>/credentialMgmt.do</url-pattern>
 <url-pattern>/createProfile.do</url-pattern>
 <url-pattern>/viewProfile.do</url-pattern>
 <url-pattern>/mdmGroup.do</url-pattern>
 </filter-mapping>
  <filter>
                <filter-name>EncodingFilter</filter-name>
                <filter-class>com.adventnet.sym.webclient.filter.EncodingFilter
↪</filter-class>
         </filter>

         <filter-mapping>
                <filter-name>EncodingFilter</filter-name>
                <url-pattern>/*</url-pattern>
                <dispatcher>FORWARD</dispatcher>
                <dispatcher>REQUEST</dispatcher>
         </filter-mapping>

 <filter>
 <filter-name>MDMI18NLocaleFilter</filter-name>
        <filter-class>com.adventnet.sym.webclient.mdm.enroll.MDMI18NLocaleFilter
```

... continues on next page ...

... continued from previous page ...

```
↪</filter-class>
    </filter>
   <filter-mapping>
 <filter-name>MDMI18NLocaleFilter</filter-name>
 <url-pattern>/mdm/enroll</url-pattern>
 <url-pattern>*.mob</url-pattern>
 <url-pattern>*.mobapps</url-pattern>
 <url-pattern>/mdm/apps</url-pattern>
 <url-pattern>/mdm/ios/acs</url-pattern>
 </filter-mapping>

 <!-- SDP-DC integration -->
 <servlet>
 <servlet-name>DCRequestHandler</servlet-name>
 <servlet-class>com.adventnet.sym.webclient.sdp.DCRequestHandler</servlet-class
↪>
 </servlet>
     <servlet-mapping>
 <servlet-name>DCRequestHandler</servlet-name>
 <url-pattern>/servlets/DCPluginServelet</url-pattern>
 </servlet-mapping>

 <servlet>
 <servlet-name>SDPDCRequestHandler</servlet-name>
 <servlet-class>com.adventnet.sym.webclient.sdp.SDPDCRequestHandler</servlet-cl
↪ass>
 </servlet>
     <servlet-mapping>
 <servlet-name>SDPDCRequestHandler</servlet-name>
 <url-pattern>/DCRequestServlet</url-pattern>
 </servlet-mapping>

 <!--SDP-DC integration -->
 <!-- Li
```

**Solution:**
**Solution type:** 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.

**Affected Software/OS**
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.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

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.

**Vulnerability Detection Method**
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: 2022-08-09T10:11:17Z

**References**
cve: CVE-2020-1938
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1
↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
url: https://www.chaitin.cn/en/ghostcat
url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances
↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://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: 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 172.16.1.8 ]

### 2.1.9 High 8009/tcp

High (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

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

**Vulnerability Detection Result**
```
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB v\x0004 Ã\x0088 \x0002OK  \x0003Â \x0007 =JSESSIONID=C960EF19D08FCE6F33F06930
↪BC435903; Path=/; HttpOnly Â \x0001 \x001Ctext/html;charset=ISO-8859-1 Â \x000
↪3 \x00041262 AB\x0004Ã²\x0003\x0004Ã®<?xml version="1.0" encoding="ISO-8859-1"
↪?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
</web-app>
 AB \x0002\x0005\x0001
```

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

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

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.

**Vulnerability Insight**
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.

**Vulnerability Detection Method**
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: `2022-08-09T10:11:17Z`

**References**
`cve: CVE-2020-1938`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1`
`↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E`
`url: https://www.chaitin.cn/en/ghostcat`
`url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487`
`url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi`
`url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances`
`↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/`
`url: https://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: 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 172.16.1.8 ]

### 2.1.10 High 8383/tcp

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

**Summary**
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     10.0.082
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.082 or later.

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.082.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: `2021-09-23T03:58:52Z`

**References**
```
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-
↪control-privilege-violation.html
```

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

**Summary**
ManageEngine Desktop Central is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     10.0.157
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: /

**Impact**
Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.157 or later.

**Affected Software/OS**
ManageEngine Desktop Central/MSP version 10.0.137 and prior.

**Vulnerability Insight**
This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure ...
OID:1.3.6.1.4.1.25623.1.0.812522
Version used: 2021-09-23T03:58:52Z

**References**
cve: CVE-2017-16924
url: https://vuldb.com/?id.113555
url: https://www.manageengine.com/desktop-management-msp/password-encryption-policy-violation.html

## High (CVSS: 9.8)
## NVT: ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability

**Summary**
ManageEngine Desktop Central is prone to an arbitrary file upload vulnerability.

**Vulnerability Detection Result**
It was possible to upload the file "/gbnvt1824434287.jsp". Please delete this file.
Vulnerable URL: https://172.16.1.8:8383/agentLogUploader?computerName=DesktopCentral&domainName=webapps&customerId=1&filename=gbnvt1824434287.jsp

**Impact**
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** VendorFix
Update to version 8.0.293 or later.

**Affected Software/OS**
ManageEngine Desktop Central prior to version 8.0.293.

**Vulnerability Insight**
The flaw in the AgentLogUploadServlet. This servlet takes input from HTTP POST and constructs an output file on the server without performing any sanitisation or even checking if the caller is authenticated.

**Vulnerability Detection Method**
Sends a crafted HTTP POST request and checks the response.
Details: `ManageEngine Desktop Central < 8.0.293 Arbitrary File Upload Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.803777
Version used: `2021-10-15T09:03:25Z`

**References**
```
cve: CVE-2013-7390
cve: CVE-2014-5007
url: http://www.exploit-db.com/exploits/29674
url: http://security-assessment.com/files/documents/advisory/DesktopCentral%20Ar
↪bitrary%20File%20Upload.pdf
```

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

**Summary**
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     10.0.092
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.092 or later.

**Affected Software/OS**
ManageEngine Desktop Central before version 10.0.092.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.092 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: `2021-09-23T03:58:52Z`

**References**
`cve: CVE-2017-11346`
`url: https://www.manageengine.com/products/desktop-central/remote-code-execution.html`

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`Vulnerable URL: https://172.16.1.8:8383/jsp/admin/DBQueryExecutor.jsp?actionFrom=getResult&query=SELECT%20*%20from%20aaauser;`

**Impact**
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

**Solution:**
**Solution type:** VendorFix
Update to version 10.0.208 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 10.0.184 and prior.

**Vulnerability Insight**
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

... continues on next page ...

... continued from previous page ...

**References**
cve: CVE-2018-5337
cve: CVE-2018-5338
cve: CVE-2018-5339
cve: CVE-2018-5341
url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln
↪erabilities-in-manageengine-desktop-central

High (CVSS: 9.8)
NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

**Summary**
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

**Vulnerability Detection Result**
It was possible to upload the file ‘https://172.16.1.8:8383/jspf/GBNVT_CVE-2015-
↪8249_test.jsp‘. Please delete this file.

**Impact**
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

**Solution:**
**Solution type:** VendorFix
Update to version 9.0.142 or later.

**Affected Software/OS**
ManageEngine Desktop Central prior to version 9.0.142.

**Vulnerability Detection Method**
Try to upload a jsp file.
Details: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi.
↪..
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: 2021-10-12T12:01:25Z

**References**
cve: CVE-2015-8249

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

**Summary**

... continues on next page ...

... continued from previous page ...

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

**Vulnerability Detection Result**

```
Vulnerable URL: https://172.16.1.8:8383/.//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>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
```

... continues on next page ...

... continued from previous page ...

```
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

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

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

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

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `'/.//WEB-INF/' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117707
Version used: `2021-10-11T08:01:31Z`

**References**

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

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

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

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

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

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2022-08-01T10:11:45Z

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2022-2226

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715

... continues on next page ...

... continued from previous page ...

```
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 172.16.1.8 ]

### 2.1.11 High 8282/tcp

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

**Product detection result**

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

**Summary**

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

**Vulnerability Detection Result**

```
The "Apache Tomcat" version on the remote host has reached the end of life.
CPE:                cpe:/a:apache:tomcat:8.0.33
Installed version:  8.0.33
Location/URL:       8282/tcp
EOL version:        8.0
EOL date:           2018-06-30
```

**Impact**

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

**Solution:**

**Solution type:** VendorFix

Update the Apache Tomcat version on the remote host to a still supported version.

**Vulnerability Detection Method**

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

Details: `Apache Tomcat End of Life (EOL) Detection (Windows)`

OID:1.3.6.1.4.1.25623.1.0.108134

Version used: `2021-02-16T13:37:32Z`

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
url: https://tomcat.apache.org/tomcat-80-eol.html
url: https://tomcat.apache.org/tomcat-60-eol.html
url: https://tomcat.apache.org/tomcat-55-eol.html
url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases
url: https://tomcat.apache.org/whichversion.html

High (CVSS: 9.1)
NVT: Apache Tomcat 'SecurityManager' 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.

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.42
Installation
path / port: 8282/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M17,
Apache Tomcat versions 8.5.0 to 8.5.11,
Apache Tomcat versions 8.0.0.RC1 to 8.0.41 and
Apache Tomcat versions 7.0.0 to 7.0.75 on Windows

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
A some calls to application listeners did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.810764
Version used: 2021-10-12T09:28:32Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2017-5648
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: http://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882b
↪f6860397368a52600@%3Cannounce.tomcat.apache.org%3E
cert-bund: CB-K18/0047
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/1060
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624

High (CVSS: 9.1)
NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windows)

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

... continues on next page ...

... continued from previous page ...

**Summary**
Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 8.0.33
Fixed version:     8.0.37
Installation
path / port:       8282/tcp
```

**Impact**
Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.

**Solution:**
**Solution type:** VendorFix
Upgrade to Apache Tomcat version 9.0.0.M10 or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, Apache Tomcat versions 8.5.0 to 8.5.4, Apache Tomcat versions 8.0.0.RC1 to 8.0.36, Apache Tomcat versions 7.0.0 to 7.0.70, and Apache Tomcat versions 6.0.0 to 6.0.45 on Windows.

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

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windo.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.811298
Version used: `2022-04-20T06:12:09Z`

**Product Detection Result**
Product: `cpe:/a:apache:tomcat:8.0.33`

... continues on next page ...

... continued from previous page ...

Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**

cve: CVE-2016-6794
cve: CVE-2016-0762
cve: CVE-2016-5018
cve: CVE-2016-6796
cve: CVE-2016-6797
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72
url: http://www.securityfocus.com/bid/93940
url: http://www.securityfocus.com/bid/93944
url: http://www.securityfocus.com/bid/93939
url: http://www.securityfocus.com/bid/93942
url: http://www.securityfocus.com/bid/93943
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8
↪.0.37
cert-bund: WID-SEC-2022-1910
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/1031
cert-bund: CB-K17/0659
cert-bund: CB-K17/0397
cert-bund: CB-K17/0133
cert-bund: CB-K16/1927
cert-bund: CB-K16/1673
cert-bund: CB-K16/1646
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: 1.3.6.1.4.1.25623.1.0.10
↪7652)

... continues on next page ...

... continued from previous page ...

**Summary**
Apache Tomcat is prone to a security bypass vulnerability.

**Vulnerability Detection Result**
`Installed version: 8.0.33`
`Fixed version: 8.0.44`
`Installation path / port: 8282/tcp`

**Impact**
Successful exploitation will allow an attacker to exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

**Solution:**
**Solution type:** VendorFix
Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.

**Affected Software/OS**
Apache Tomcat 9.0.0.M1 to 9.0.0.M20, Apache Tomcat 8.5.0 to 8.5.14, Apache Tomcat 8.0.0.RC1 to 8.0.43 and Apache Tomcat 7.0.0 to 7.0.77 on Windows

**Vulnerability Insight**
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

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811140
Version used: `2022-04-13T11:57:07Z`

**Product Detection Result**
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-5664
url: https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b
↪8b7896538478d76066@%3Cannounce.tomcat.apache.org%3E
url: http://www.securityfocus.com/bid/98888
cert-bund: CB-K18/0605
cert-bund: CB-K18/0603
cert-bund: CB-K18/0478
cert-bund: CB-K18/0066
cert-bund: CB-K18/0047
cert-bund: CB-K17/2024
cert-bund: CB-K17/2017
cert-bund: CB-K17/1831
cert-bund: CB-K17/1748
cert-bund: CB-K17/1492
cert-bund: CB-K17/1423
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/0977
dfn-cert: DFN-CERT-2018-1274
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0513
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-2116
dfn-cert: DFN-CERT-2017-2106
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1827
dfn-cert: DFN-CERT-2017-1558
dfn-cert: DFN-CERT-2017-1485
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.

**Vulnerability Detection Result**

```
Installed version: 8.0.33
```

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| Fixed version: | 8.0.39 |
| Installation path / port: | 8282/tcp |

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

**Solution:**
**Solution type:** VendorFix
Upgrade to version 9.0.0.M17, 8.5.11 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M11 to 9.0.0.M15 and Apache Tomcat versions 8.5.0 to 8.5.9 on Windows.

**Vulnerability Insight**
The refactoring to make wider use of ByteBuffer introduced a regression that could cause information to leak between requests on the same connection. When running behind a reverse proxy, this could result in information leakage between users.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.810719
Version used: 2022-04-13T11:57:07Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2016-8747
url: http://svn.apache.org/viewvc?view=revision&revision=1774161
url: http://www.securityfocus.com/bid/96895
url: http://svn.apache.org/viewvc?view=revision&revision=1774166
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.11
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M17
cert-bund: CB-K17/0426
dfn-cert: DFN-CERT-2017-0433

High (CVSS: 7.5)
NVT: Apache Tomcat NIO HTTP connector 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.

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.41
Installation
path / port: 8282/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M13, Apache Tomcat versions 8.5.0 to 8.5.8, Apache Tomcat versions 8.0.0.RC1 to 8.0.39, Apache Tomcat versions 7.0.0 to 7.0.73, and Apache Tomcat versions 6.0.16 to 6.0.48 on Windows.

**Vulnerability Insight**
The flaw exists due to error handling of the send file code for the NIO HTTP connector in Apache Tomcat resulting in the current Processor object being added to the Processor cache multiple times. This in turn means that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.811296
Version used: 2022-04-13T11:57:07Z

**Product Detection Result**
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)

**References**

cve: CVE-2016-8745
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60409
url: http://www.securityfocus.com/bid/94828
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0303
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1929
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
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 'pipelined' Requests 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.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.43
Installation
path / port: 8282/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M18, Apache Tomcat versions 8.5.0 to 8.5.12, Apache Tomcat versions 8.0.0.RC1 to 8.0.42, Apache Tomcat versions 7.0.0 to 7.0.76 and Apache Tomcat versions 6.0.0 to 6.0.52 on Windows.

**Vulnerability Insight**
A bug in the handling of the pipelined requests when send file was used resulted in the pipelined request being lost when send file processing of the previous request completed.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Window.
↪..
OID:1.3.6.1.4.1.25623.1.0.810762
Version used: 2021-10-12T09:28:32Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2017-5647
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: http://tomcat.apache.org/security-6.html
url: https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0
↪dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E
cert-bund: CB-K18/0047

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1831
cert-bund: CB-K17/1423
cert-bund: CB-K17/1246
cert-bund: CB-K17/1205
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1485
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1243
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624
```

High (CVSS: 7.5)
NVT: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability (Windows)

**Product detection result**

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

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 8.0.33
Fixed version:     8.0.52
Installation
path / port:       8282/tcp
```

**Impact**

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

**Solution:**

**Solution type:** VendorFix

Upgrade to Apache Tomcat version 9.0.8 or 8.5.31 or 8.0.52 or 7.0.90 or later. Please see the references for more information.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

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.

**Vulnerability Insight**
The flaw exists due to improper handing of overflow in the UTF-8 decoder with supplementary characters.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813724
Version used: `2021-10-11T09:46:29Z`

**Product Detection Result**
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
`cve: CVE-2018-1336`
`url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201`
`↪80722090435.GA60759%40minotaur.apache.org%3E`
`url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52`
`cert-bund: CB-K18/0809`
`dfn-cert: DFN-CERT-2020-0048`
`dfn-cert: DFN-CERT-2018-2474`
`dfn-cert: DFN-CERT-2018-2165`
`dfn-cert: DFN-CERT-2018-2142`
`dfn-cert: DFN-CERT-2018-2133`
`dfn-cert: DFN-CERT-2018-2125`
`dfn-cert: DFN-CERT-2018-2097`
`dfn-cert: DFN-CERT-2018-1928`
`dfn-cert: DFN-CERT-2018-1753`
`dfn-cert: DFN-CERT-2018-1541`
`dfn-cert: DFN-CERT-2018-1471`
`dfn-cert: DFN-CERT-2018-1443`
`dfn-cert: DFN-CERT-2018-1262`

High (CVSS: 7.5)
NVT: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows

**Product detection result**
`cpe:/a:apache:tomcat:8.0.33`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`

... continues on next page ...

... continued from previous page ...

↪7652)

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

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.36
Installation
path / port: 8282/tcp

**Impact**
Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).

**Solution:**
**Solution type:** VendorFix
Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.

**Affected Software/OS**
Apache Tomcat 7.x before 7.0.70, 8.0.0.RC1 before 8.0.36, 8.5.x before 8.5.3, and 9.0.0.M1 before 9.0.0.M7.

**Vulnerability Insight**
The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.808197
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2016-3092
url: http://tomcat.apache.org/security-7.html
url: http://www.securityfocus.com/bid/91453
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-9.html

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1537
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1750
cert-bund: CB-K17/1198
cert-bund: CB-K17/1060
cert-bund: CB-K17/0657
cert-bund: CB-K17/0397
cert-bund: CB-K16/1993
cert-bund: CB-K16/1799
cert-bund: CB-K16/1758
cert-bund: CB-K16/1322
cert-bund: CB-K16/1002
cert-bund: CB-K16/0993
dfn-cert: DFN-CERT-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.

**Vulnerability Detection Result**

```
Installed version: 8.0.33
Fixed version:     8.0.53
Installation
path / port:       8282/tcp
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.

**Solution:**
**Solution type:** VendorFix
Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52 and 7.0.35 to 7.0.88 on Windows.

**Vulnerability Insight**
The flaw exists due to a missing host name verification when using TLS with the WebSocket client.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813742
Version used: `2021-10-11T09:46:29Z`

**Product Detection Result**
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
`cve: CVE-2018-8034`
`url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201`
`↪80722091057.GA70283@minotaur.apache.org%3E`
`url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32`
`url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90`
`cert-bund: CB-K19/0907`
`cert-bund: CB-K19/0616`
`cert-bund: CB-K19/0320`
`cert-bund: CB-K18/1005`
`cert-bund: CB-K18/0809`
`dfn-cert: DFN-CERT-2019-2418`
`dfn-cert: DFN-CERT-2019-1627`
`dfn-cert: DFN-CERT-2019-1237`
`dfn-cert: DFN-CERT-2019-0951`
`dfn-cert: DFN-CERT-2019-0451`

... continues on next page ...

... continued from previous page ...

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: 7.1)
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: 1.3.6.1.4.1.25623.1.0.10
↪7652)

**Summary**
Apache Tomcat is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.39
Installation
path / port: 8282/tcp

**Impact**
Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.

**Solution:**
**Solution type:** VendorFix
Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M11, Apache Tomcat versions 8.5.0 to 8.5.6, Apache Tomcat versions 8.0.0.RC1 to 8.0.38, Apache Tomcat versions 7.0.0 to 7.0.72, and Apache Tomcat versions 6.0.0 to 6.0.47 on Windows.

**Vulnerability Insight**
The code that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

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: 2022-04-13T11:57:07Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2016-6816
url: https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48
url: http://www.securityfocus.com/bid/94461
url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13
url: https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-
↪information-disclosure
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0198
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1976
cert-bund: CB-K16/1927
cert-bund: CB-K16/1815
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0203
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-2090
dfn-cert: DFN-CERT-2016-2035
dfn-cert: DFN-CERT-2016-1922

[ return to 172.16.1.8 ]

### 2.1.12 High 3306/tcp

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.39
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.39, 8.0.30 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.38 and prior and 8.0 through 8.0.29.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.148511
Version used: 2022-07-22T10:11:18Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2022-1292
cve: CVE-2022-27778
cve: CVE-2018-25032
cve: CVE-2022-21515
url: https://www.oracle.com/security-alerts/cpujul2022.html#AppendixMSQL
advisory-id: cpujul2022
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1772

... continues on next page ...

... continued from previous page ...

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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1310
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1049
dfn-cert: DFN-CERT-2022-0986
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716
```

High (CVSS: 9.8)
NVT: Oracle Mysql Security Update (cpuoct2018 - 02) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

**Solution:**

**Solution type:** VendorFix

The vendor has released updates. Please see the references for more information.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

Oracle MySQL version 5.5.x through 5.5.61, 5.6.x through 5.6.41, 5.7.x through 5.7.23 and 8.0.x through 8.0.12.

**Vulnerability Insight**
Multiple flaws exist due to:
- An unspecified error within 'InnoDB (zlib)' component of MySQL Server.
- An unspecified error within 'Server: Parser' component of MySQL Server.
- An unspecified error within 'Client programs' component of MySQL Server.
- An unspecified error within 'Server: Storage Engines' component of MySQL Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Update (cpuoct2018 - 02) - Windows`
OID:1.3.6.1.4.1.25623.1.0.814258
Version used: `2022-06-24T09:38:38Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2018-3133`
`cve: CVE-2018-3174`
`cve: CVE-2018-3282`
`cve: CVE-2016-9843`
`cve: CVE-2016-9840`
`cve: CVE-2016-9841`
`cve: CVE-2016-9842`
`url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL`
`advisory-id: cpuoct2018`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0714`
`cert-bund: CB-K18/1005`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K18/0030`
`cert-bund: CB-K17/2199`
`cert-bund: CB-K17/2168`
`cert-bund: CB-K17/1745`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1622`
`cert-bund: CB-K17/1585`
`cert-bund: CB-K17/1062`
`cert-bund: CB-K17/0877`
`cert-bund: CB-K17/0784`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1996
dfn-cert: DFN-CERT-2020-1536
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2273
dfn-cert: DFN-CERT-2018-2110
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2016-2109
```

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (cpuoct2016) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation of this vulnerability will allow a remote user to access restricted data.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.52 and prior, 5.6 through 5.6.33 and 5.7 through 5.7.15.

**Vulnerability Insight**
Multiple flaws exist due to multiple unspecified errors in the 'Server: Security: Encryption' and 'Server: Logging' components.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809386
Version used: `2021-10-13T11:01:26Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2016-5584`
`cve: CVE-2016-6662`
`cve: CVE-2016-7440`
`url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL`
`advisory-id: cpuoct2016`
`url: http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution`
`↪-Privesc-CVE-2016-6662.txt`
`url: https://www.exploit-db.com/exploits/40360/`
`cert-bund: CB-K17/0139`
`cert-bund: CB-K17/0055`
`cert-bund: CB-K16/1846`
`cert-bund: CB-K16/1755`
`cert-bund: CB-K16/1742`
`cert-bund: CB-K16/1714`
`cert-bund: CB-K16/1655`
`cert-bund: CB-K16/1624`
`cert-bund: CB-K16/1448`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1392
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1753
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1540
dfn-cert: DFN-CERT-2016-1479

High (CVSS: 9.8)
NVT: Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.36
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.36, 8.0.27 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.35 and prior and 8.0 through 8.0.26.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117741
Version used: 2021-10-23T08:58:44Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

cve: CVE-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: https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixMSQL
advisory-id: cpuoct2021
cert-bund: WID-SEC-2022-2000
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1515
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0874
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0473
cert-bund: CB-K22/0469
cert-bund: CB-K22/0316
cert-bund: CB-K22/0224

... continues on next page ...

... continued from previous page ...

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-2022-2825
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0867
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0122
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

... continues on next page ...

... continued from previous page ...

```
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: MySQL / MariaDB weak password

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

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

**Vulnerability Detection Result**

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

**Solution:**

**Solution type:** Mitigation

Change the password as soon as possible.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Details: `MySQL / MariaDB weak password`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `2021-02-10T08:19:07Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

High (CVSS: 9.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version: Apply the patch`

**Impact**
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced vendor advisory or upgrade to the latest version.

**Affected Software/OS**
Oracle MySQL version 5.1.x to 5.1.64 and Oracle MySQL version 5.5.x to 5.5.26 on Windows.

**Vulnerability Insight**
The flaws are due to multiple unspecified errors in MySQL server component related to server replication, information schema, protocol and server optimizer.

**Vulnerability Detection Method**
Details: `Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.803111
Version used: 2022-04-27T12:01:52Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

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

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.38
Installation
path / port: 3306/tcp

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

... continues on next page ...

... continued from previous page ...

Update to version 5.7.38, 8.0.29 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.37 and prior and 8.0 through 8.0.28.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.37 / 8.0 <= 8.0.28 Security Update (cpuapr2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.113944
Version used: `2022-04-25T14:30:15Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2022-0778`
`cve: CVE-2022-21454`
`cve: CVE-2022-21417`
`cve: CVE-2022-21427`
`cve: CVE-2022-21451`
`cve: CVE-2022-21444`
`cve: CVE-2022-21460`
`url: https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixMSQL`
`advisory-id: cpuapr2022`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-1081`
`cert-bund: WID-SEC-2022-1057`
`cert-bund: WID-SEC-2022-0836`
`cert-bund: WID-SEC-2022-0833`
`cert-bund: WID-SEC-2022-0826`
`cert-bund: WID-SEC-2022-0767`
`cert-bund: WID-SEC-2022-0677`
`cert-bund: WID-SEC-2022-0551`
`cert-bund: WID-SEC-2022-0530`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0393`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: WID-SEC-2022-0270`
`cert-bund: WID-SEC-2022-0261`
`cert-bund: WID-SEC-2022-0200`

... continues on next page ...

... continued from previous page ...

```
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-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1928
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1667
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1370
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1205
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
```

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.49
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.49 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.48 and prior.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.48 Security Update (cpujul2020) - Windows
OID:1.3.6.1.4.1.25623.1.0.144286
Version used: 2021-08-16T12:00:57Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2020-1967
cve: CVE-2020-14539
cve: CVE-2020-14559
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL
advisory-id: cpujul2020
cert-bund: CB-K21/1088
cert-bund: CB-K21/0070
cert-bund: CB-K20/1023
cert-bund: CB-K20/1017
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

... continues on next page ...

... continued from previous page ...

```
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 Feb17 (Windows)

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.6.21
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation of this vulnerability will allow attackers to cause crash of applications using that MySQL client.

**Solution:**

**Solution type:** VendorFix

Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.

**Affected Software/OS**

Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Windows

**Vulnerability Insight**

Multiple errors exist as,

... continues on next page ...

... continued from previous page ...

- In sql-common/client.c script 'mysql_prune_stmt_list' function, the for loop adds elements to pruned_list without removing it from the existing list.
- If application gets disconnected just before it tries to prepare a new statement, 'mysql_prune_stmt_list' tries to detach all previously prepared statements.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.810603
Version used: 2021-10-12T09:28:32Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2017-3302
url: https://bugs.mysql.com/bug.php?id=63363
url: https://bugs.mysql.com/bug.php?id=70429
url: http://www.openwall.com/lists/oss-security/2017/02/11/11
cert-bund: CB-K18/0224
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430

High (CVSS: 7.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

... continues on next page ...

... continued from previous page ...

Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20`

**Impact**
Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server version 5.5.40 and earlier, and 5.6.21 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Server:-Security:Encryption, InnoDB:DML, Replication, and Security:Privileges:Foreign Key.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805132
Version used: `2022-04-14T06:42:08Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2015-0411`
`cve: CVE-2014-6568`
`cve: CVE-2015-0382`
`cve: CVE-2015-0381`
`cve: CVE-2015-0374`
`url: http://secunia.com/advisories/62525`
`url: http://www.securityfocus.com/bid/72191`
`url: http://www.securityfocus.com/bid/72210`
`url: http://www.securityfocus.com/bid/72200`
`url: http://www.securityfocus.com/bid/72214`
`url: http://www.securityfocus.com/bid/72227`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html`
`cert-bund: CB-K15/1193`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.5.40
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

**Solution:**

**Solution type:** VendorFix

Update to version 5.5.40, 5.6.21 or later.

**Affected Software/OS**

Oracle MySQL Server versions 5.5.39 and prior and 5.6 through 5.6.20.

**Vulnerability Insight**

Unspecified errors in the MySQL Server component via unknown vectors related to C API SSL CERTIFICATE HANDLING, SERVER:DML, SERVER:SSL:yaSSL, SERVER:OPTIMIZER, SERVER:INNODB DML FOREIGN KEYS.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.39 / 5.6 <= 5.6.20 Security Update (cpuoct2014) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804781
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-6507`
`cve: CVE-2014-6491`
`cve: CVE-2014-6500`
`cve: CVE-2014-6469`
`cve: CVE-2014-6555`
`cve: CVE-2014-6559`
`cve: CVE-2014-6494`
`cve: CVE-2014-6496`
`cve: CVE-2014-6464`
`url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/70444`
`url: http://www.securityfocus.com/bid/70446`
`url: http://www.securityfocus.com/bid/70451`
`url: http://www.securityfocus.com/bid/70469`
`url: http://www.securityfocus.com/bid/70478`
`url: http://www.securityfocus.com/bid/70487`
`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`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1357

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

**Vulnerability Insight**
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Option' sub-component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujul2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.808591
Version used: 2022-07-07T10:16:06Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

```
cve: CVE-2016-3471
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91913
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169
```

High (CVSS: 7.5)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation of this vulnerability will allow remote attackers to cause the affected application to crash, resulting in a denial-of-service condition.

**Solution:**

**Solution type:** VendorFix

Apply the patch from the referenced advisory.

**Affected Software/OS**

Oracle MySQL version 5.5.54 and earlier, 5.6.20 and earlier on Windows

**Vulnerability Insight**

The flaw exists due to some unspecified error in the 'Server: C API' component due to failure to handle exceptional conditions.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows
OID:1.3.6.1.4.1.25623.1.0.810880
Version used: 2022-04-13T11:57:07Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2017-3302
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/96162
cert-bund: CB-K18/0224
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430

High (CVSS: 7.4)
NVT: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.34
Installation

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.34, 8.0.24 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.33 and prior and 8.0 through 8.0.23.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145796
Version used: 2021-08-26T14:01:06Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-3449
cve: CVE-2021-3450
cve: CVE-2021-23840
cve: CVE-2021-23841
cve: CVE-2021-2307
cve: CVE-2021-2304
cve: CVE-2021-2180
cve: CVE-2021-2194
cve: CVE-2021-2166
cve: CVE-2021-2179
cve: CVE-2021-2226
cve: CVE-2021-2169
cve: CVE-2021-2146
cve: CVE-2021-2174
cve: CVE-2021-2171
cve: CVE-2021-2162
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
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

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0671
cert-bund: WID-SEC-2022-0669
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K22/0476
cert-bund: CB-K22/0061
cert-bund: CB-K21/1097
cert-bund: CB-K21/1095
cert-bund: CB-K21/1065
cert-bund: CB-K21/0785
cert-bund: CB-K21/0770
cert-bund: CB-K21/0573
cert-bund: CB-K21/0572
cert-bund: CB-K21/0565
cert-bund: CB-K21/0421
cert-bund: CB-K21/0412
cert-bund: CB-K21/0409
cert-bund: CB-K21/0389
cert-bund: CB-K21/0317
cert-bund: CB-K21/0185
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2197
dfn-cert: DFN-CERT-2021-2196
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1825
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
```

... continues on next page ...

... continued from previous page ...

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

High (CVSS: 7.2)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-06 Oct15 (Windows)

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server Server 5.5.44 and earlier, and 5.6.25 and earlier

**Vulnerability Insight**
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-06 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805769
Version used: `2022-04-14T06:42:08Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2015-4879`
`cve: CVE-2015-4819`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html`
`url: http://www.securityfocus.com/bid/77140`
`url: http://www.securityfocus.com/bid/77196`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0493`
`cert-bund: CB-K16/0246`
`cert-bund: CB-K16/0245`
`cert-bund: CB-K15/1844`
`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`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a vulnerability in the parser.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.30
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.30, 8.0.20 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.29 and prior and 8.0 through 8.0.19.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.29 / 8.0 <= 8.0.19 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145800
Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-2144
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021

... continues on next page ...

... continued from previous page ...

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

High (CVSS: 7.2)
NVT: Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.52
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an remote attacker to gain elevated privileges on the affected system, also could allow buffer overflow attacks.

**Solution:**
**Solution type:** VendorFix
Upgrade to Oracle MySQL Server 5.5.52 or later.

**Affected Software/OS**
Oracle MySQL Server 5.5.x to 5.5.51 on windows

**Vulnerability Insight**
Multiple errors exist. Please see the references for more information.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)
OID:1.3.6.1.4.1.25623.1.0.809300
Version used: 2021-10-15T11:13:32Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**
url: http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html

High (CVSS: 7.2)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.46 and prior, 5.6 through 5.6.27 and version 5.7.9.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 / 5.7.9 Security Update (cpujan20.
↪..
OID:1.3.6.1.4.1.25623.1.0.806876
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

cve: CVE-2016-0609
cve: CVE-2016-0608
cve: CVE-2016-0606
cve: CVE-2016-0600
cve: CVE-2016-0598
cve: CVE-2016-0597
cve: CVE-2016-0546
cve: CVE-2016-0505
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81258
url: http://www.securityfocus.com/bid/81226
url: http://www.securityfocus.com/bid/81188
url: http://www.securityfocus.com/bid/81182
url: http://www.securityfocus.com/bid/81151
url: http://www.securityfocus.com/bid/81066
url: http://www.securityfocus.com/bid/81088
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0143
dfn-cert: DFN-CERT-2016-0104

High (CVSS: 7.1)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpujan2019) - Windows

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

**Solution:**
**Solution type:** VendorFix
Updates are available. Apply the necessary patch from the referenced link.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

**Vulnerability Insight**
The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.
For further information refer to the official advisory via the referenced link.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.112489
Version used: 2021-09-07T14:01:38Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2019-2534

... continues on next page ...

... continued from previous page ...

cve: CVE-2019-2529
cve: CVE-2019-2482
cve: CVE-2019-2455
cve: CVE-2019-2503
cve: CVE-2018-0734
cve: CVE-2019-2537
cve: CVE-2019-2481
cve: CVE-2019-2507
cve: CVE-2019-2531
cve: CVE-2018-5407
url: https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL
advisory-id: cpujan2019
cert-bund: WID-SEC-2022-1696
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K22/0045
cert-bund: CB-K20/0324
cert-bund: CB-K20/0136
cert-bund: CB-K19/1121
cert-bund: CB-K19/0696
cert-bund: CB-K19/0622
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0318
cert-bund: CB-K19/0316
cert-bund: CB-K19/0314
cert-bund: CB-K19/0050
cert-bund: CB-K19/0044
cert-bund: CB-K18/1173
cert-bund: CB-K18/1065
cert-bund: CB-K18/1039
dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2305
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1600
dfn-cert: DFN-CERT-2019-1588

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0782
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0778
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0232
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2019-0103
dfn-cert: DFN-CERT-2019-0102
dfn-cert: DFN-CERT-2018-2541
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2513
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2444
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2360
dfn-cert: DFN-CERT-2018-2338
dfn-cert: DFN-CERT-2018-2214
```

High (CVSS: 7.1)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service attack and partially modify data.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.19 and earlier on Windows

**Vulnerability Insight**
The flaw exists due to an error in 'Server:Partition' component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.812650
Version used: `2022-07-04T10:18:32Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2018-2562`
`url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html`
`cert-bund: CB-K18/0480`
`cert-bund: CB-K18/0392`
`cert-bund: CB-K18/0265`
`cert-bund: CB-K18/0096`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-1265`
`dfn-cert: DFN-CERT-2018-0733`
`dfn-cert: DFN-CERT-2018-0515`
`dfn-cert: DFN-CERT-2018-0424`
`dfn-cert: DFN-CERT-2018-0286`
`dfn-cert: DFN-CERT-2018-0101`

High (CVSS: 7.0)
NVT: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (cpuoct2016) - Windows

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of these vulnerabilities will allow remote authenticated attackers to cause denial of service conditions and gain elevated privileges.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.51 and prior, 5.6 through 5.6.32 and 5.7 through 5.7.14.

**Vulnerability Insight**
Multiple flaws exist due to multiple unspecified errors in the 'Server:GIS', 'Server:Federated', 'Server:Optimizer', 'Server:Types', 'Server:Error Handling' and 'Server:MyISAM' components.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.51 / 5.6 <= 5.6.32 / 5.7 <= 5.7.14 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.809372
Version used: 2021-10-13T11:01:26Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-3492
cve: CVE-2016-5626
cve: CVE-2016-5629

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-5616
cve: CVE-2016-5617
cve: CVE-2016-8283
cve: CVE-2016-6663
cve: CVE-2016-6664
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0139
cert-bund: CB-K16/1979
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2016-2089
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714
```

[ return to 172.16.1.8 ]

### 2.1.13 Medium 4848/tcp

Medium (CVSS: 5.8)
NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

**Summary**
The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

**Vulnerability Detection Result**

```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
------------------------------------------------------------------------------
↪----------------------------------------------
TLSv1.0          | 2
TLSv1.1          | 2
TLSv1.2          | 2
```

**Impact**

... continues on next page ...

... continued from previous page ...

A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
General solution options are:
- remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service
- enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service

**Affected Software/OS**
The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)`
OID:1.3.6.1.4.1.25623.1.0.117758
Version used: `2021-11-15T10:28:20Z`

**References**
`cve: CVE-2009-3555`
`url: https://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html`
`url: https://www.g-sec.lu/practicaltls.pdf`
`url: https://www.kb.cert.org/vuls/id/120541`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://lwn.net/Articles/362234/`
`url: https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385`
`url: https://datatracker.ietf.org/doc/html/rfc5746`
`url: https://mailarchive.ietf.org/arch/msg/tls/Y1O3HUcq9T94rMLCGPTTozURtSI/`
`cert-bund: CB-K17/1878`
`cert-bund: CB-K17/1642`
`cert-bund: CB-K15/0637`
`dfn-cert: DFN-CERT-2017-1960`
`dfn-cert: DFN-CERT-2017-1722`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0613
dfn-cert: DFN-CERT-2011-1720
dfn-cert: DFN-CERT-2011-1138
dfn-cert: DFN-CERT-2011-1137
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0700
dfn-cert: DFN-CERT-2011-0321
dfn-cert: DFN-CERT-2011-0193
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2011-0181
dfn-cert: DFN-CERT-2011-0116
dfn-cert: DFN-CERT-2011-0021
dfn-cert: DFN-CERT-2011-0020
dfn-cert: DFN-CERT-2011-0019
dfn-cert: DFN-CERT-2010-1762
dfn-cert: DFN-CERT-2010-1731
dfn-cert: DFN-CERT-2010-1710
dfn-cert: DFN-CERT-2010-1702
dfn-cert: DFN-CERT-2010-1650
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1527
dfn-cert: DFN-CERT-2010-1500
dfn-cert: DFN-CERT-2010-1439
dfn-cert: DFN-CERT-2010-1424
dfn-cert: DFN-CERT-2010-1406
dfn-cert: DFN-CERT-2010-1405
dfn-cert: DFN-CERT-2010-1387
dfn-cert: DFN-CERT-2010-1385
dfn-cert: DFN-CERT-2010-1380
dfn-cert: DFN-CERT-2010-1368
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-1227
dfn-cert: DFN-CERT-2010-1052
dfn-cert: DFN-CERT-2010-1009
dfn-cert: DFN-CERT-2010-1000
dfn-cert: DFN-CERT-2010-0899
dfn-cert: DFN-CERT-2010-0859
dfn-cert: DFN-CERT-2010-0833
dfn-cert: DFN-CERT-2010-0815
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0729
dfn-cert: DFN-CERT-2010-0725
dfn-cert: DFN-CERT-2010-0707

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0669
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0619
dfn-cert: DFN-CERT-2010-0618
dfn-cert: DFN-CERT-2010-0603
dfn-cert: DFN-CERT-2010-0586
dfn-cert: DFN-CERT-2010-0579
dfn-cert: DFN-CERT-2010-0562
dfn-cert: DFN-CERT-2010-0558
dfn-cert: DFN-CERT-2010-0544
dfn-cert: DFN-CERT-2010-0539
dfn-cert: DFN-CERT-2010-0525
dfn-cert: DFN-CERT-2010-0504
dfn-cert: DFN-CERT-2010-0498
dfn-cert: DFN-CERT-2010-0491
dfn-cert: DFN-CERT-2010-0488
dfn-cert: DFN-CERT-2010-0485
dfn-cert: DFN-CERT-2010-0456
dfn-cert: DFN-CERT-2010-0455
dfn-cert: DFN-CERT-2010-0451
dfn-cert: DFN-CERT-2010-0413
dfn-cert: DFN-CERT-2010-0411
dfn-cert: DFN-CERT-2010-0410
dfn-cert: DFN-CERT-2010-0407
dfn-cert: DFN-CERT-2010-0406
dfn-cert: DFN-CERT-2010-0405
dfn-cert: DFN-CERT-2010-0388
dfn-cert: DFN-CERT-2010-0370
dfn-cert: DFN-CERT-2010-0339
dfn-cert: DFN-CERT-2010-0303
dfn-cert: DFN-CERT-2010-0273
dfn-cert: DFN-CERT-2010-0201
dfn-cert: DFN-CERT-2010-0166
dfn-cert: DFN-CERT-2010-0050
dfn-cert: DFN-CERT-2010-0030
dfn-cert: DFN-CERT-2009-1833
dfn-cert: DFN-CERT-2009-1821
dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

**Impact**
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:

... continues on next page ...

... continued from previous page ...

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2021-11-15T10:28:20Z

**References**
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://orchilles.com/ssl-renegotiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

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

**Vulnerability Detection Result**
```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)                | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)              | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
```

... continues on next page ...

... continued from previous page ...

```
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

**Impact**
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

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

**Vulnerability Detection Method**
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Vulnerability Detection Result**

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`
`cert-bund: CB-K15/0365`
`cert-bund: CB-K15/0364`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[ return to 172.16.1.8 ]

### 2.1.14 Medium 135/tcp

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

**Summary**

... continues on next page ...

... continued from previous page ...

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

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49154]
     Annotation: Impl friendly name
Port: 49177/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49177]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49179/tcp
```

... continues on next page ...

... continued from previous page ...

```
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.16.1.8[49179]
Port: 49244/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.8[49244]
     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:172.16.1.8[49244]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

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

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[ return to 172.16.1.8 ]

### 2.1.15 Medium 8022/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**
The flaw allows to inject client-side script into Desktop Centrals web page.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: `2022-04-13T07:21:45Z`

**References**
`cve: CVE-2018-8722`
`url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-`
`↪vulnerability.html`
`url: http://www.securityfocus.com/bid/103426`

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

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

**Vulnerability Detection Result**
`The following input fields where identified (URL:input name):`
`http://172.16.1.8:8022/configurations.do:j_password`

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

**Solution:**
**Solution type:** Workaround

... continues on next page ...

... continued from previous page ...

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

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

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

Medium (CVSS: 4.3)
NVT: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

**Summary**
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: `2021-09-23T03:58:52Z`

**References**
`url: https://packetstormsecurity.com/files/136463`

[ return to 172.16.1.8 ]

### 2.1.16 Medium 8020/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The flaw allows to inject client-side script into Desktop Centrals web page.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: `2022-04-13T07:21:45Z`

**References**
`cve: CVE-2018-8722`
`url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-vulnerability.html`
`url: http://www.securityfocus.com/bid/103426`

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

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

**Vulnerability Detection Result**

```
Vulnerable URL: http://172.16.1.8:8020/WEB-INf./web.xml
Response (truncated):
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/
 ns/j2ee/web-app_2_4.xsd" version="2.4">
<!-- $Id$ -->
 <!-- Added for MickeyClient Pdf Generation -->
 <context-param>
 <param-name>ContextPath</param-name>
 <param-value>/</param-value>
 </context-param>
 <context-param>
 <param-name>defaultSkin</param-name>
 <param-value>woody</param-value>
 </context-param>
 <context-param>
 <param-name>useInstantFeedback</param-name>
 <param-value>true</param-value>
 </context-param>
 <context-param>
 <param-name>mailServerName</param-name>
 <param-value>smtp.india.adventnet.com</param-value>
 </context-param>
 <context-param>
```

... continues on next page ...

... continued from previous page ...

```
 <param-name>instantFeedbackAddress</param-name>
 <param-value>sym-issues@adventnet.com</param-value>
 </context-param>
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

**Solution:**
**Solution type:** VendorFix
Please contact the vendor for more information on possible fixes.

**Affected Software/OS**
The following products are known to be affected:
- A misconfigured reverse proxy.
Other products might be affected as well.

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

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)
OID:1.3.6.1.4.1.25623.1.0.117225
Version used: 2021-10-06T12:27:36Z

**References**
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

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

**Vulnerability Detection Result**
Vulnerable URL: http://172.16.1.8:8020/WEB-INF../web.xml
Response (truncated):

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

... continues on next page ...

... continued from previous page ...

```
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

**Solution:**
**Solution type:** VendorFix
Please contact the vendor for more information on possible fixes.

**Affected Software/OS**
The following products are known to be affected:
- Apache 1.3.29 + Resin 2.1.12
Other products might be affected as well.

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

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INF../' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117221

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-13T07:21:45Z

**References**
cve: CVE-2004-0281
url: http://marc.info/?l=bugtraq&m=107635084830547&w=2
url: http://www.securityfocus.com/bid/9617

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

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

**Vulnerability Detection Result**
The following input fields where identified (URL:input name):
http://172.16.1.8:8020/configurations.do:j_password

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

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

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

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2020-08-24T15:18:35Z

**References**
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se

... continues on next page ...

... continued from previous page ...

↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

**Summary**
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**
Installed version: 9.1.084
Fixed version: 9.2.026
Installation
path / port: /

**Impact**
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: 2021-09-23T03:58:52Z

**References**
url: https://packetstormsecurity.com/files/136463

[ return to 172.16.1.8 ]

### 2.1.17 Medium 3000/tcp

Medium (CVSS: 6.5)
NVT: Ruby on Rails < 6.0.3.2 DoS Vulnerability

**Summary**
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
```
Installed version: 4.1.1
Fixed version:     6.0.3.2
Installation
path / port:       /
```

**Impact**
Successful exploitation would allow an attacker to render legitimate users unable to use the application.

**Solution:**
**Solution type:** VendorFix
Update to version 6.0.3.2.

**Affected Software/OS**
Ruby on Rails through version 6.0.3.1.

**Vulnerability Insight**
An untrusted user may run any pending migration in production.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails < 6.0.3.2 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113716
Version used: `2021-07-07T11:00:41Z`

**References**
```
cve: CVE-2020-8185
url: https://hackerone.com/reports/899069
cert-bund: CB-K20/0604
dfn-cert: DFN-CERT-2021-0842
dfn-cert: DFN-CERT-2020-2327
```

Medium (CVSS: 6.1)
NVT: Ruby on Rails Action View Cross Site Scripting Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**

. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 4.1.1
Fixed version:     4.2.7.1
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow a remote attacker to inject arbitrary web script or HTML via crafted parameters.

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 3.2.22.3 or 4.2.7.1 or 5.0.0.1 or later.

**Affected Software/OS**
Ruby on Rails 3.x before 3.2.22.3, Ruby on Rails 4.x before 4.2.7.1 and Ruby on Rails 5.x before 5.0.0.1 on Windows.

**Vulnerability Insight**
The flaw is due to the Text declared as 'HTML safe' when passed as an attribute value to a tag helper will not have quotes escaped which can lead to an XSS attack.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Action View Cross Site Scripting Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807379
Version used: `2022-04-13T13:17:10Z`

**References**

```
cve: CVE-2016-6316
url: http://seclists.org/oss-sec/2016/q3/260
url: http://www.securityfocus.com/bid/92430
url: https://groups.google.com/forum/#!msg/rubyonrails-security/I-VWr034ouk/gGu2
↪FrCwDAAJ
url: http://weblog.rubyonrails.org/2016/8/11/Rails-5-0-0-1-4-2-7-2-and-3-2-22-3-
↪have-been-released
cert-bund: CB-K17/1730
cert-bund: CB-K16/1256
dfn-cert: DFN-CERT-2017-1809
dfn-cert: DFN-CERT-2016-1321
```

Medium (CVSS: 5.9)
NVT: Ruby on Rails Information Disclosure Vulnerability (GHSA-rmj8-8hhh-gv5h) - Windows

**Summary**
Ruby on Rails is prone to an information disclosure vulnerability in puma.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 4.1.1
Fixed version: 5.2.6.2
Installation
path / port: /

**Solution:**
**Solution type:** VendorFix
Update to version 5.2.6.2, 6.0.4.6, 6.1.4.6, 7.0.2.2 or later.

**Affected Software/OS**
Ruby on Rails version 5.x through 7.0.x.

**Vulnerability Insight**
Puma may not always call close on the response body. Rails depends on the response body being closed in order for its CurrentAttributes implementation to work correctly.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Information Disclosure Vulnerability (GHSA-rmj8-8hhh-gv5h) - Wind.
↪..
OID:1.3.6.1.4.1.25623.1.0.147673
Version used: 2022-02-24T03:03:30Z

**References**
cve: CVE-2022-23634
url: https://github.com/advisories/GHSA-rmj8-8hhh-gv5h
dfn-cert: DFN-CERT-2022-1898
dfn-cert: DFN-CERT-2022-1891
dfn-cert: DFN-CERT-2022-1506
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1195
dfn-cert: DFN-CERT-2022-1187
dfn-cert: DFN-CERT-2022-0992

Medium (CVSS: 5.3)
NVT: Ruby on Rails Acrive Model Security Bypass Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a security bypass vulnerability.

**Vulnerability Detection Result**
Installed version: 4.1.1
Fixed version: 4.1.14.1

... continues on next page ...

... continued from previous page ...

Installation
path / port: /

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

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

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

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

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Acrive Model Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.809360
Version used: 2022-04-13T13:17:10Z

**References**
cve: CVE-2016-0753
url: http://www.openwall.com/lists/oss-security/2016/01/25/14
url: http://www.securityfocus.com/bid/82247
cert-bund: CB-K16/0625
cert-bund: CB-K16/0254
cert-bund: CB-K16/0238
cert-bund: CB-K16/0236
cert-bund: CB-K16/0166
cert-bund: CB-K16/0165
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0272
dfn-cert: DFN-CERT-2016-0259
dfn-cert: DFN-CERT-2016-0258
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2016-0178

Medium (CVSS: 5.3)
NVT: Ruby on Rails Acrive Record Security Bypass Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to security bypass vulnerabilities.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 4.1.1
Fixed version: 4.1.14.1
Installation
path / port: /

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

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 3.2.22.1 or 4.1.14.1 or 4.2.5.1, or later.

**Affected Software/OS**
Ruby on Rails before 3.1.x and 3.2.x before 3.2.22.1, Ruby on Rails 4.0.x and 4.1.x before 4.1.14.1 and Ruby on Rails 4.2.x before 4.2.5.1 on Windows.

**Vulnerability Insight**
The flaw is due to the script 'activerecord/lib/active_record/nested_attributes.rb' does not properly implement a certain destroy option.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Acrive Record Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.809358
Version used: 2022-04-13T13:17:10Z

**References**
cve: CVE-2015-7577
url: http://www.openwall.com/lists/oss-security/2016/01/25/10
url: http://www.securityfocus.com/bid/81806
cert-bund: CB-K17/0278
cert-bund: CB-K16/0625
cert-bund: CB-K16/0419
cert-bund: CB-K16/0254
cert-bund: CB-K16/0166
cert-bund: CB-K16/0165
dfn-cert: DFN-CERT-2017-0284
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0272
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2016-0178

Medium (CVSS: 5.3)
NVT: Ruby on Rails Action View 'render' Directory Traversal Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a directory traversal vulnerability.

**Vulnerability Detection Result**
```
Installed version: 4.1.1
Fixed version:     4.1.14.2
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow a remote attacker to read arbitrary files by leveraging an application's unrestricted use of the render method.

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 3.2.22.2 or 4.1.14.2 or later.

**Affected Software/OS**
Ruby on Rails before 3.2.22.2, Ruby on Rails 4.x before 4.1.14.2 on Windows.

**Vulnerability Insight**
The flaw is due to an improper validation of crafted requests to action view, one of the components of action pack.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Action View 'render' Directory Traversal Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809354
Version used: `2022-04-13T13:17:10Z`

**References**
```
cve: CVE-2016-2097
url: https://www.debian.org/security/2016/dsa-3509
url: http://www.securityfocus.com/bid/83726
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/ly-IH-
↪fxr_Q/WLoOhcMZIAAJ
cert-bund: WID-SEC-2022-2271
cert-bund: CB-K16/0522
cert-bund: CB-K16/0419
cert-bund: CB-K16/0372
dfn-cert: DFN-CERT-2022-2796
dfn-cert: DFN-CERT-2016-0566
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0404
```

Medium (CVSS: 5.0)
NVT: Ruby on Rails Active Support Denial of Service Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
```
Installed version: 4.1.1
Fixed version:     4.1.11
Installation
path / port:       /
```

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

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 4.1.11, 4.2.2 or later.

**Affected Software/OS**
Ruby on Rails before 4.1.11 and Ruby on Rails 4.2.x before 4.2.2 on Windows.

**Vulnerability Insight**
The flaw is due to Specially crafted XML documents can cause applications to raise a SystemStackError and potentially cause a denial of service attack.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Active Support Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807383
Version used: `2021-10-15T11:13:32Z`

**References**
```
cve: CVE-2015-3227
url: http://openwall.com/lists/oss-security/2015/06/16/16
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/bahr2J
↪Lnxvk/x4EocXnHPp8J
cert-bund: CB-K16/0166
cert-bund: CB-K15/1056
cert-bund: CB-K15/0856
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2015-1111
dfn-cert: DFN-CERT-2015-0899
```

Medium (CVSS: 4.3)
NVT: Ruby on Rails Active Support Cross Site Scripting Vulnerability (Windows)

**Summary**
Ruby on Rails is prone to a cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**
```
Installed version: 4.1.1
Fixed version:     4.1.11
Installation
path / port:       /
```

**Impact**
Successful exploitation will allow a remote attacker to inject arbitrary web script or HTML via crafted parameters.

**Solution:**
**Solution type:** VendorFix
Upgrade to Ruby on Rails 4.2.2, 4.1.11 or later.

**Affected Software/OS**
Ruby on Rails versions 3.x, 3.0.x, 3.1.x, 3.2.x, 4.1.x before 4.1.11, 4.2.x before 4.2.2 on Linux.

**Vulnerability Insight**
The flaw is due to error in handling 'ActiveSupport::JSON.encode' method which can lead to an XSS attack.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Active Support Cross Site Scripting Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807381
Version used: `2021-10-15T11:13:32Z`

**References**
```
cve: CVE-2015-3226
url: http://openwall.com/lists/oss-security/2015/06/16/17
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/7VlB_p
↪ck3hU/3QZrGIaQW6cJ
cert-bund: CB-K16/0166
cert-bund: CB-K15/0856
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2015-0899
```

Medium (CVSS: 4.3)
NVT: Ruby on Rails < 5.2.5, 6.x < 6.0.4 CSRF Vulnerability

. . . continues on next page . . .

... continued from previous page ...

**Summary**
Ruby on Rails is prone to a cross-site request forgery (CSRF) vulnerability.

**Vulnerability Detection Result**
`Installed version: 4.1.1`
`Fixed version: 5.2.5`
`Installation path / port: /`

**Impact**
Successful exploitation would allow an authenticated attacer to perform actions in the context of another user.

**Solution:**
**Solution type:** VendorFix
Update to version 5.2.5 or 6.0.4 respectively.

**Affected Software/OS**
Ruby on Rails through version 5.2.4 and versions 6.0.0 through 6.0.3.

**Vulnerability Insight**
An attacker can use a global CSRF token, as can be found in the authenticity_token meta tag, to forge form-specific CSRF tokens.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails < 5.2.5, 6.x < 6.0.4 CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113714
Version used: `2021-07-07T11:00:41Z`

**References**
`cve: CVE-2020-8166`
`url: https://hackerone.com/reports/732415`
`cert-bund: CB-K20/0477`
`dfn-cert: DFN-CERT-2021-0842`
`dfn-cert: DFN-CERT-2020-2327`
`dfn-cert: DFN-CERT-2020-2093`

[ return to 172.16.1.8 ]

### 2.1.18 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)

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

**Summary**
openssh is prone to a security bypass vulnerability.

**Vulnerability Detection Result**
Installed version: 7.1
Fixed version: 7.6
Installation
path / port: 22/tcp

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

**Solution:**
**Solution type:** VendorFix
Upgrade to OpenSSH version 7.6 or later.

**Affected Software/OS**
OpenSSH versions before 7.6 on Windows

**Vulnerability Insight**
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: 2022-08-22T10:11:10Z

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

**References**
cve: CVE-2017-15906
url: https://www.openssh.com/txt/release-7.6

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/101552
url: https://github.com/openbsd/src/commit/a6981567e8e
cert-bund: CB-K20/0041
cert-bund: CB-K18/0137
cert-bund: CB-K17/2126
cert-bund: CB-K17/2014
cert-bund: CB-K17/2002
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2017-2217
dfn-cert: DFN-CERT-2017-2100
dfn-cert: DFN-CERT-2017-2093
```

Medium (CVSS: 5.3)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows

**Product detection result**

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

**Summary**

OpenSSH is prone to a user enumeration vulnerability.

**Vulnerability Detection Result**

```
Installed version: 7.1
Fixed version:     None
Installation
path / port:       22/tcp
```

**Impact**

Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

**Solution:**

**Solution type:** WillNotFix

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

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

OpenSSH version 5.9 through 7.8.

**Vulnerability Insight**
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813887
Version used: `2021-05-28T07:06:21Z`

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

**References**
`cve: CVE-2018-15919`
`url: https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`url: https://seclists.org/oss-sec/2018/q3/180`
`cert-bund: CB-K18/0885`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2191`

Medium (CVSS: 5.3)
NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows

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

**Summary**
OpenSSH is prone to a user enumeration vulnerability.

**Vulnerability Detection Result**
```
Installed version: 7.1
Fixed version:     7.8
Installation
path / port:       22/tcp
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

**Solution:**
**Solution type:** VendorFix
Update to version 7.8 or later.

**Affected Software/OS**
OpenSSH versions 7.7 and prior.

**Vulnerability Insight**
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.8 User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2021-10-11T09:46:29Z`

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

**References**
`cve: CVE-2018-15473`
`url: https://0day.city/cve-2018-15473.html`
`url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d`
`↪1e0`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K18/1031`
`cert-bund: CB-K18/0873`
`dfn-cert: DFN-CERT-2021-2178`
`dfn-cert: DFN-CERT-2020-2189`
`dfn-cert: DFN-CERT-2020-0228`
`dfn-cert: DFN-CERT-2019-2046`
`dfn-cert: DFN-CERT-2019-0857`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2259`
`dfn-cert: DFN-CERT-2018-2191`
`dfn-cert: DFN-CERT-2018-1806`
`dfn-cert: DFN-CERT-2018-1696`

[ return to 172.16.1.8 ]

### 2.1.19 Medium 9200/tcp

Medium (CVSS: 6.8)
NVT: Elastisearch Remote Code Execution Vulnerability

**Summary**
Elasticsearch is prone to a remote-code-execution vulnerability.

**Vulnerability Detection Result**
`Vulnerable URL: http://172.16.1.8:9200/_search?source=%7B%22size%22%3A1%2C%22que`
`↪ry%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%7D`
`↪%7D%2C%22script_fields%22%3A%7B%22VTTest%22%3A%7B%22script%22%3A%22import%20ja`
`↪va.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2Fwin`
`↪dows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D`
`↪%7D%7D&callback=?`

**Impact**
An attacker can exploit this issue to execute arbitrary code

**Solution:**
**Solution type:** VendorFix
Ask the vendor for an update or disable 'dynamic scripting'

**Affected Software/OS**
Elasticsearch < 1.2

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

**Vulnerability Detection Method**
Send a special crafted HTTP GET request and check the response
Details: `Elastisearch Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105032
Version used: `2022-12-05T10:11:03Z`

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

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

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

**Vulnerability Detection Result**
`Installed version: 1.1.1`
`Fixed version: 6.8.17`
`Installation path / port: /`

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.17, 7.13.3 or later.

**Affected Software/OS**
Elasticsearch prior to version 6.8.17 and 7.x prior to 7.13.3.

**Vulnerability Insight**
An uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)`
OID:1.3.6.1.4.1.25623.1.0.146386
Version used: `2021-08-17T12:00:57Z`

**References**
`cve: CVE-2021-22144`
`url: https://discuss.elastic.co/t/elasticsearch-7-13-3-and-6-8-17-security-updat`
`↪e/278100`
`cert-bund: WID-SEC-2022-1777`
`dfn-cert: DFN-CERT-2022-2315`

Medium (CVSS: 6.5)
NVT: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability (Windows)

**Summary**
Elasticsearch is prone to a field disclosure vulnerability.

**Vulnerability Detection Result**
`Installed version: 1.1.1`
`Fixed version: 6.8.12`

... continues on next page ...

... continued from previous page ...

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

**Impact**
An attacker could gain additional permissions against a restricted index.

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.12, 7.9.1 or later.

**Affected Software/OS**
Elasticsearch prior to version 6.8.12 and 7.9.0.

**Vulnerability Insight**
A field disclosure flaw was found in Elasticsearch when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.144431
Version used: `2021-07-07T11:00:41Z`

**References**
`cve: CVE-2020-7019`
`url: https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update`
`↪/245456`

Medium (CVSS: 5.9)
NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) (Windows)

**Summary**
Elasticsearch is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**

```
Installed version: 1.1.1
Fixed version:     6.8.2
Installation
path / port:       /
```

**Impact**

... continues on next page ...

... continued from previous page ...

On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.2 or 7.2.1 respectively.

**Affected Software/OS**
Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.

**Vulnerability Insight**
A race condition flaw was found in the response headers Elasticsearch returns to a request.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability. ↪..`
OID:1.3.6.1.4.1.25623.1.0.117162
Version used: `2021-08-30T11:01:18Z`

**References**
`cve: CVE-2019-7614`
`url: https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/ ↪192963`
`url: https://www.elastic.co/community/security/`

Medium (CVSS: 5.3)
NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)

**Summary**
Elasticsearch is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 1.1.1
Fixed version:     6.8.15
Installation
path / port:       /
```

**Impact**
This could lead to disclosing the existence of documents and fields the attacker should not be able to view or result in an attacker gaining additional insight into potentially sensitive indices.

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.15, 7.12.0 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Elasticsearch versions prior to versions 6.8.15 or 7.12.0.

**Vulnerability Insight**
The following vulnerabilities exist:
- CVE-2021-22135: Suggester & Profile API information disclosure flaw
- CVE-2021-22137: Field disclosure flaw

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)`
OID:1.3.6.1.4.1.25623.1.0.145940
Version used: `2021-08-17T12:00:57Z`

**References**
`cve: CVE-2021-22135`
`cve: CVE-2021-22137`
`url: https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updat`
`↪e/268125`
`cert-bund: WID-SEC-2022-0720`

Medium (CVSS: 4.9)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)

**Summary**
Elasticsearch is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
```
Installed version: 1.1.1
Fixed version:     6.8.14
Installation
path / port:       /
```

**Impact**
This could allow an Elasticsearch administrator to view sensitive details.

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.14, 7.10.0 or later.

**Affected Software/OS**
Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
Elasticsearch has an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)`
OID:1.3.6.1.4.1.25623.1.0.145383
Version used: `2021-08-17T12:00:57Z`

**References**
`cve: CVE-2020-7021`
`url: https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-updat`
`↪e/263915`
`url: https://www.elastic.co/community/security`

Medium (CVSS: 4.3)
NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)

**Summary**
Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**
`Installed version: 1.1.1`
`Fixed version: 1.4.0.Beta1`

**Impact**
Successful exploitation will allow remote attackers to inject arbitrary web script or HTML.

**Solution:**
**Solution type:** VendorFix
Update to Elasticsearch version 1.4.0.Beta1, or later.

**Affected Software/OS**
Elasticsearch version 1.3.x and prior on Windows.

**Vulnerability Insight**
The Flaw is due to an error in the CORS functionality.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808092
Version used: `2022-04-13T13:17:10Z`

... continues on next page ...

... continued from previous page ...

**References**
cve: CVE-2014-6439
url: https://www.elastic.co/community/security/
url: http://www.securityfocus.com/bid/70233
url: http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded

[ return to 172.16.1.8 ]

### 2.1.20 Medium 8181/tcp

Medium (CVSS: 5.8)
NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

**Summary**
The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

**Vulnerability Detection Result**
```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.0          | 2
TLSv1.1          | 2
TLSv1.2          | 2
```

**Impact**
A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
General solution options are:
- remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service
- enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service

**Affected Software/OS**
The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)
OID:1.3.6.1.4.1.25623.1.0.117758
Version used: 2021-11-15T10:28:20Z

**References**
cve: CVE-2009-3555
url: https://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html
url: https://www.g-sec.lu/practicaltls.pdf
url: https://www.kb.cert.org/vuls/id/120541
url: https://orchilles.com/ssl-renegotiation-dos/
url: https://lwn.net/Articles/362234/
url: https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385
url: https://datatracker.ietf.org/doc/html/rfc5746
url: https://mailarchive.ietf.org/arch/msg/tls/Y1O3HUcq9T94rMLCGPTTozURtSI/
cert-bund: CB-K17/1878
cert-bund: CB-K17/1642
cert-bund: CB-K15/0637
dfn-cert: DFN-CERT-2017-1960
dfn-cert: DFN-CERT-2017-1722
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0613
dfn-cert: DFN-CERT-2011-1720
dfn-cert: DFN-CERT-2011-1138
dfn-cert: DFN-CERT-2011-1137
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0700
dfn-cert: DFN-CERT-2011-0321
dfn-cert: DFN-CERT-2011-0193
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2011-0181
dfn-cert: DFN-CERT-2011-0116
dfn-cert: DFN-CERT-2011-0021
dfn-cert: DFN-CERT-2011-0020
dfn-cert: DFN-CERT-2011-0019
dfn-cert: DFN-CERT-2010-1762

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2010-1731
dfn-cert: DFN-CERT-2010-1710
dfn-cert: DFN-CERT-2010-1702
dfn-cert: DFN-CERT-2010-1650
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1527
dfn-cert: DFN-CERT-2010-1500
dfn-cert: DFN-CERT-2010-1439
dfn-cert: DFN-CERT-2010-1424
dfn-cert: DFN-CERT-2010-1406
dfn-cert: DFN-CERT-2010-1405
dfn-cert: DFN-CERT-2010-1387
dfn-cert: DFN-CERT-2010-1385
dfn-cert: DFN-CERT-2010-1380
dfn-cert: DFN-CERT-2010-1368
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-1227
dfn-cert: DFN-CERT-2010-1052
dfn-cert: DFN-CERT-2010-1009
dfn-cert: DFN-CERT-2010-1000
dfn-cert: DFN-CERT-2010-0899
dfn-cert: DFN-CERT-2010-0859
dfn-cert: DFN-CERT-2010-0833
dfn-cert: DFN-CERT-2010-0815
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0729
dfn-cert: DFN-CERT-2010-0725
dfn-cert: DFN-CERT-2010-0707
dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0669
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0619
dfn-cert: DFN-CERT-2010-0618
dfn-cert: DFN-CERT-2010-0603
dfn-cert: DFN-CERT-2010-0586
dfn-cert: DFN-CERT-2010-0579
dfn-cert: DFN-CERT-2010-0562
dfn-cert: DFN-CERT-2010-0558
dfn-cert: DFN-CERT-2010-0544
dfn-cert: DFN-CERT-2010-0539
dfn-cert: DFN-CERT-2010-0525
dfn-cert: DFN-CERT-2010-0504
dfn-cert: DFN-CERT-2010-0498
dfn-cert: DFN-CERT-2010-0491
dfn-cert: DFN-CERT-2010-0488
dfn-cert: DFN-CERT-2010-0485
dfn-cert: DFN-CERT-2010-0456

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2010-0455
dfn-cert: DFN-CERT-2010-0451
dfn-cert: DFN-CERT-2010-0413
dfn-cert: DFN-CERT-2010-0411
dfn-cert: DFN-CERT-2010-0410
dfn-cert: DFN-CERT-2010-0407
dfn-cert: DFN-CERT-2010-0406
dfn-cert: DFN-CERT-2010-0405
dfn-cert: DFN-CERT-2010-0388
dfn-cert: DFN-CERT-2010-0370
dfn-cert: DFN-CERT-2010-0339
dfn-cert: DFN-CERT-2010-0303
dfn-cert: DFN-CERT-2010-0273
dfn-cert: DFN-CERT-2010-0201
dfn-cert: DFN-CERT-2010-0166
dfn-cert: DFN-CERT-2010-0050
dfn-cert: DFN-CERT-2010-0030
dfn-cert: DFN-CERT-2009-1833
dfn-cert: DFN-CERT-2009-1821
dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
`The following indicates that the remote SSL/TLS service is affected:`

... continues on next page ...

... continued from previous page ...

```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2021-11-15T10:28:20Z`

**References**
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`cert-bund: CB-K17/0980`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

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

**Vulnerability Detection Result**

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)              | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)            | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                        | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 04A9972F
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)  | None
valid from                       | 2013-05-15 05:33:38 UTC
valid until                      | 2023-05-13 05:33:38 UTC
```

**Impact**
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

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

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Vulnerability Detection Result**
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274

... continues on next page ...

... continued from previous page ...

Version used: 2021-07-19T08:11:48Z

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884

... 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
```

[ return to 172.16.1.8 ]

### 2.1.21 Medium 3389/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

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

**Vulnerability Detection Result**
```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

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

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)

... continues on next page ...

... continued from previous page ...

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

**Vulnerability Detection Method**

Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2021-12-01T13:10:37Z

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Vulnerability Detection Result**
`The service is only providing the deprecated TLSv1.0 protocol and supports one o ↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S ↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.`

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2012-0638

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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

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

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=vagrant-2008R2
Signature Algorithm:  sha1WithRSAEncryption
```

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

... 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/`

[ return to 172.16.1.8 ]

### 2.1.22 Medium 8383/tcp

Medium (CVSS: 6.1)
NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

**Summary**
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**
The flaw allows to inject client-side script into Desktop Centrals web page.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: `2022-04-13T07:21:45Z`

**References**
`cve: CVE-2018-8722`
`url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-vulnerability.html`
`url: http://www.securityfocus.com/bid/103426`

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Vulnerability Detection Result**
```
The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleasanton,ST=CA,C=US (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

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

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

**Vulnerability Detection Result**
The certificate of the remote service expired on 2020-09-05 12:24:44.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 701E2E6DF8854C4F0B298DFF03A2C6F0BAC7D315 |
| fingerprint (SHA-256) | C1DF756862FA17582C31E8F8EBDA084D1A1341815B716E↪B135AD83CD7B01A5A5 |
| 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 |

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

... continues on next page ...

... continued from previous page ...

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

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0)
NVT: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)

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

**Vulnerability Detection Result**
Vulnerable URL: https://172.16.1.8:8383/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>
```

... continues on next page ...

... continued from previous page ...

```
 <context-param>
 <param-name>AUTO_IMPORT_USER</param-name>
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

**Solution:**
**Solution type:** VendorFix
Please contact the vendor for more information on possible fixes.

**Affected Software/OS**
The following products are known to be affected:
- Apache 1.3.29 + Resin 2.1.12
Other products might be affected as well.

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

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.

... continues on next page ...

... continued from previous page ...

Details: '/WEB-INF../' Information Disclosure Vulnerability (HTTP)
OID:1.3.6.1.4.1.25623.1.0.117221
Version used: 2022-04-13T07:21:45Z

**References**
cve: CVE-2004-0281
url: http://marc.info/?l=bugtraq&m=107635084830547&w=2
url: http://www.securityfocus.com/bid/9617

Medium (CVSS: 5.0)
NVT: '/WEB-INf./' Information Disclosure Vulnerability (HTTP)

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

**Vulnerability Detection Result**
Vulnerable URL: https://172.16.1.8:8383/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>
```

... continues on next page ...

... continued from previous page ...

```
 <param-value>false</param-value>
 </context-param>
 <context-param>
                <param-name>PARAMETER-ENCODING</param-name>
                <param-value>UTF-8</param-value>
 </context-param>
 <listener>
 <listener-class>com.adventnet.sym.webclient.configurations.SyMHttpSessionBindi
↪ngListener</listener-class>
 </listener>
 <!-- SDP-DC integration -->
    <listener>
 <listener-class>com.adventnet.sym.webclient.common.DCSessionListener</listener
↪-class>
    </listener>
   <!-- SDP-DC integra
```

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

**Solution:**
**Solution type:** VendorFix
Please contact the vendor for more information on possible fixes.

**Affected Software/OS**
The following products are known to be affected:
- A misconfigured reverse proxy.
Other products might be affected as well.

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

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `'/WEB-INf./' Information Disclosure Vulnerability (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.117225
Version used: `2021-10-06T12:27:36Z`

... continues on next page ...

... continued from previous page ...

**References**
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60667

Medium (CVSS: 4.3)
NVT: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

**Summary**
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

**Vulnerability Detection Result**
Installed version: 9.1.084
Fixed version: 9.2.026
Installation
path / port: /

**Impact**
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

**Solution:**
**Solution type:** VendorFix
Update to version 9.2.026 or later.

**Affected Software/OS**
ManageEngine Desktop Central version 9.1.099 and prior.

**Vulnerability Insight**
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: 2021-09-23T03:58:52Z

**References**
url: https://packetstormsecurity.com/files/136463

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**

... continues on next page ...

... continued from previous page ...

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Vulnerability Detection Result**

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**

Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

**References**

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

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

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

**Vulnerability Detection Result**
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E
↪7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleas
↪anton,ST=CA,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

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

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

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

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

[ return to 172.16.1.8 ]

### 2.1.23 Medium 8282/tcp

Medium (CVSS: 5.9)
NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities (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 multiple access bypass vulnerabilities.

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.0.50
Installation
path / port: 8282/tcp

**Impact**
Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.

**Solution:**
**Solution type:** VendorFix
Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.

**Affected Software/OS**
Apache Tomcat versions 9.0.0.M1 to 9.0.4
Apache Tomcat versions 8.5.0 to 8.5.27
Apache Tomcat versions 8.0.0.RC1 to 8.0.49
Apache Tomcat versions 7.0.0 to 7.0.84 on Windows.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
Multiple flaws are due to:
- The system does not properly enforce security constraints that defined by annotations of Servlets in certain cases, depending on the order that Servlets are loaded.
- The URL pattern of " (the empty string) which exactly maps to the context root was not correctly handled when used as part of a security constraint definition.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit.
↪..
OID:1.3.6.1.4.1.25623.1.0.812784
Version used: 2022-04-13T07:21:45Z

**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
↪7e10949b01b1f8a0fb@%3Cannounce.tomcat.apache.org%3E
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

... continues on next page ...

... continued from previous page ...

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: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

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

**Vulnerability Detection Result**
The following URLs requires Basic Authentication (URL:realm name):
http://172.16.1.8:8282/host-manager/html:"Tomcat Host Manager Application"
http://172.16.1.8:8282/manager/html:"Tomcat Manager Application"
http://172.16.1.8:8282/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)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2020-08-24T15:18:35Z

... continues on next page ...

... continued from previous page ...

**References**
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: Apache Tomcat Open Redirect 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**
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.

**Vulnerability Detection Result**
Installed version: 8.0.33
Fixed version: 8.5.34

**Solution:**
**Solution type:** VendorFix
Update to version 7.0.91, 8.5.34, 9.0.12 or later.

**Affected Software/OS**
Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Open Redirect Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.141569
Version used: 2021-06-14T11:00:34Z

**Product Detection Result**
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

**References**
cve: CVE-2018-11784

... continues on next page ...

... continued from previous page ...

```
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
cert-bund: 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 172.16.1.8 ]

### 2.1.24 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.5.28
Installation
path / port:       3306/tcp
```

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

... continues on next page ...

... continued from previous page ...

Update to version 5.1.66, 5.5.28 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.1.65 and prior and 5.5 through 5.5.27.

**Vulnerability Insight**
The flaw allows remote authenticated users to affect availability, related to GIS Extension.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117201
Version used: `2021-02-12T11:09:59Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2012-5060`
`url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL`
`advisory-id: cpujan2013`
`dfn-cert: DFN-CERT-2013-0079`

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 5.5.20
Fixed version:     5.5.24
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

**Impact**
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'InnoDB' package / privilege.

**Solution:**
**Solution type:** VendorFix
Update to version 5.5.24 or later.

**Affected Software/OS**
Oracle MySQL Server 5.5.x through 5.5.23.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117267
Version used: `2021-03-18T11:53:07Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2012-1735`
`cve: CVE-2012-1757`
`cve: CVE-2012-1756`
`url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL`
`advisory-id: cpujul2012`
`dfn-cert: DFN-CERT-2012-1389`

## Medium (CVSS: 6.8)
## NVT: MySQL Server Components Multiple Unspecified Vulnerabilities

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20-log`

... continues on next page ...

... continued from previous page ...

Fixed version: See advisory

**Impact**
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
MySQL version 5.1.x before 5.1.62 and 5.5.x before 5.5.22.

**Vulnerability Insight**
Multiple unspecified errors exist in the Server Optimizer and Server DML components.

**Vulnerability Detection Method**
Details: MySQL Server Components Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.803808
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-1690
cve: CVE-2012-1688
cve: CVE-2012-1703
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53058
url: http://www.securityfocus.com/bid/53067
url: http://www.securityfocus.com/bid/53074
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1170
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0936
dfn-cert: DFN-CERT-2012-0933
dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.67, 5.5.29 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117203
Version used: 2021-02-12T11:09:59Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-5611
cve: CVE-2013-0384
cve: CVE-2013-0389
cve: CVE-2013-0385
cve: CVE-2013-0375
cve: CVE-2012-1702
cve: CVE-2013-0383
cve: CVE-2012-0572

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2012-0574
cve: CVE-2012-1705
cve: CVE-2012-4414
url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL
advisory-id: cpujan2013
cert-bund: CB-K13/0919
cert-bund: CB-K13/0603
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1597
dfn-cert: DFN-CERT-2013-0259
dfn-cert: DFN-CERT-2013-0192
dfn-cert: DFN-CERT-2013-0119
dfn-cert: DFN-CERT-2013-0118
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2013-0079
dfn-cert: DFN-CERT-2013-0037
dfn-cert: DFN-CERT-2013-0028
dfn-cert: DFN-CERT-2012-2285
dfn-cert: DFN-CERT-2012-2258
dfn-cert: DFN-CERT-2012-2215
dfn-cert: DFN-CERT-2012-2200
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.5.29
Installation
path / port:       3306/tcp
```

**Solution:**

**Solution type:** VendorFix

Update to version 5.5.29 or later.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server versions 5.5 through 5.5.28.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117205
Version used: `2021-02-12T11:09:59Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2012-5612`
`cve: CVE-2013-0386`
`cve: CVE-2013-0368`
`cve: CVE-2013-0371`
`cve: CVE-2012-0578`
`cve: CVE-2013-0367`
`cve: CVE-2012-5096`
`url: https://www.oracle.com/security-alerts/cpujan2013.html#AppendixMSQL`
`advisory-id: cpujan2013`
`dfn-cert: DFN-CERT-2013-0259`
`dfn-cert: DFN-CERT-2013-0079`

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server Multiple Vulnerabilities-02 Nov12 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`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).

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** VendorFix
Apply the patch from the references or upgrade to latest version.

**Affected Software/OS**
Oracle MySQL version 5.1.x to 5.1.65 and Oracle MySQL version 5.5.x to 5.5.27 on Windows.

**Vulnerability Insight**
The flaws are due to multiple unspecified errors in MySQL server component related to server installation and server optimizer.

**Vulnerability Detection Method**
Details: `Oracle MySQL Server Multiple Vulnerabilities-02 Nov12 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803112
Version used: `2022-04-27T12:01:52Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2012-3180`
`cve: CVE-2012-3177`
`cve: CVE-2012-3160`
`url: http://secunia.com/advisories/51008/`
`url: http://www.securityfocus.com/bid/56003`
`url: http://www.securityfocus.com/bid/56005`
`url: http://www.securityfocus.com/bid/56027`
`url: http://www.securelist.com/en/advisories/51008`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html`
`url: https://support.oracle.com/rs?type=doc&id=1475188.1`
`dfn-cert: DFN-CERT-2012-2200`
`dfn-cert: DFN-CERT-2012-2118`

Medium (CVSS: 6.6)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version: Apply the patch`
`Installation path / port: 3306/tcp`

**Impact**
Successful exploitation of this vulnerability will allow remote attackers to have impact on availability, confidentiality and integrity.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier, 5.7.17 and earlier on Windows

**Vulnerability Insight**
Multiple flaws exist due to multiple unspecified errors in the 'Server: DML', 'Server: Optimizer', 'Server: Thread Pooling', 'Client mysqldump', 'Server: Security: Privileges' components of the application.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810882
Version used: `2022-07-20T10:33:02Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2017-3309`
`cve: CVE-2017-3308`
`cve: CVE-2017-3329`
`cve: CVE-2017-3456`
`cve: CVE-2017-3453`
`cve: CVE-2017-3600`
`cve: CVE-2017-3462`

... continues on next page ...

... continued from previous page ...

cve: CVE-2017-3463
cve: CVE-2017-3461
cve: CVE-2017-3464
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97742
url: http://www.securityfocus.com/bid/97725
url: http://www.securityfocus.com/bid/97763
url: http://www.securityfocus.com/bid/97831
url: http://www.securityfocus.com/bid/97776
url: http://www.securityfocus.com/bid/97765
url: http://www.securityfocus.com/bid/97851
url: http://www.securityfocus.com/bid/97849
url: http://www.securityfocus.com/bid/97812
url: http://www.securityfocus.com/bid/97818
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1563
cert-bund: CB-K17/1401
cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/0927
cert-bund: CB-K17/0657
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1630
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0675

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.37 and earlier and 5.6.17 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to SRINFOSC and SRCHAR.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804722
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-4258`
`cve: CVE-2014-4260`
`url: http://secunia.com/advisories/59521`
`url: http://www.securityfocus.com/bid/68564`
`url: http://www.securityfocus.com/bid/68573`
`url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi`
`↪ty_patches`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A`
`↪ppendixMSQL`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/0891`
`cert-bund: CB-K14/0868`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-0930`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-0911

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow remote to compromise availability confidentiality, and integrity of the system.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.19 and earlier on Windows.

**Vulnerability Insight**
Multiple flaws exist due to:
- An error in 'Client programs' component.
- An error in 'Server: DDL'.
- An error in 'Server: Replication'

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.811991
Version used: 2022-07-21T10:11:30Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log

... continues on next page ...

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

cve: CVE-2017-10379
cve: CVE-2017-10384
cve: CVE-2017-10268
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101415
url: http://www.securityfocus.com/bid/101406
url: http://www.securityfocus.com/bid/101390
cert-bund: CB-K18/0480
cert-bund: CB-K18/0242
cert-bund: CB-K18/0224
cert-bund: CB-K17/2048
cert-bund: CB-K17/1748
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0260
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-2137
dfn-cert: DFN-CERT-2017-1827

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation of this vulnerability will allow remote attackers to compromise availability of the system.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.11 and earlier on Windows.

**Vulnerability Insight**
The flaw exists due to an error in 'Server: Optimizer'

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811986
Version used: `2022-07-21T10:11:30Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2017-10378`
`url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html`
`url: http://www.securityfocus.com/bid/101375`
`cert-bund: CB-K18/0480`
`cert-bund: CB-K18/0242`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/2048`
`cert-bund: CB-K17/1748`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-1265`
`dfn-cert: DFN-CERT-2018-0515`
`dfn-cert: DFN-CERT-2018-0260`
`dfn-cert: DFN-CERT-2018-0242`
`dfn-cert: DFN-CERT-2017-2137`
`dfn-cert: DFN-CERT-2017-1827`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.67, 5.5.29 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpuapr2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.803459
Version used: 2022-07-21T10:11:30Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-1531
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.68, 5.5.30, 5.6.11 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.1.67 and prior, 5.5 through 5.5.29 and 5.6 through 5.6.10.

**Vulnerability Insight**
Unspecified error in some unknown vectors related to Information Schema.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.117206
Version used: 2022-07-21T10:11:30Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2013-2378
cve: CVE-2013-1506
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59188
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.68, 5.5.30 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.1.67 and prior and 5.5 through 5.5.29.

**Vulnerability Insight**
Unspecified error in Server Partition and in some unspecified vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117209

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-1521
cve: CVE-2013-1552
cve: CVE-2013-1555
cve: CVE-2012-5614
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59196
url: http://www.securityfocus.com/bid/59210
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.69, 5.5.31, 5.6.11 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL Server versions 5.1.68 and prior, 5.5 through 5.5.30 and 5.6 through 5.6.10.

**Vulnerability Insight**
Unspecified error in Server Optimizer, Server Privileges, InnoDB, and in some unspecified vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117207
Version used: `2022-07-21T10:11:30Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-2375`
`cve: CVE-2013-1544`
`cve: CVE-2013-1532`
`cve: CVE-2013-2389`
`cve: CVE-2013-2392`
`cve: CVE-2013-2391`
`url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/59207`
`url: http://www.securityfocus.com/bid/59209`
`url: http://www.securityfocus.com/bid/59224`
`url: http://www.securityfocus.com/bid/59242`
`advisory-id: cpuapr2013`
`dfn-cert: DFN-CERT-2013-0882`
`dfn-cert: DFN-CERT-2013-0839`
`dfn-cert: DFN-CERT-2013-0798`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.31 and prior and 5.6 through 5.6.11.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806878
Version used: `2022-09-12T10:18:03Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
```
cve: CVE-2016-0502
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81136
advisory-id: cpujan2016
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-0266
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0104

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.39
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

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

**Affected Software/OS**
Oracle MySQL Server versions 5.5.38 and prior and 5.6 through 5.6.19.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to CLIENT:MYSQLADMIN, CLIENT:MYSQLDUMP, SERVER:MEMORY STORAGE ENGINE, SERVER:SSL:yaSSL, SERVER:DML, SERVER:SSL:yaSSL, SERVER:REPLICATION ROW FORMAT BINARY LOG DML, SERVER:CHARACTER SETS, and SERVER:MyISAM.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.38 / 5.6 <= 5.6.19 Security Update (cpuoct2014) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.804782
Version used: 2021-02-12T11:09:59Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2014-6530
cve: CVE-2012-5615
cve: CVE-2014-6495
cve: CVE-2014-6478
cve: CVE-2014-4274
cve: CVE-2014-4287
cve: CVE-2014-6484
cve: CVE-2014-6505
cve: CVE-2014-6463
cve: CVE-2014-6551
url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL
advisory-id: cpuoct2014
cert-bund: CB-K15/1518
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K14/1482
cert-bund: CB-K14/1420
cert-bund: CB-K14/1412
cert-bund: CB-K14/1299
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2014-1567
dfn-cert: DFN-CERT-2014-1500
dfn-cert: DFN-CERT-2014-1489
dfn-cert: DFN-CERT-2014-1357
dfn-cert: DFN-CERT-2013-0259

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple denial-of-service vulnerabilities.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows

**Vulnerability Insight**
Multiple flaws exist due to:
- An error in the 'Server: DDL' component.
- Multiple errors in the 'Server: Optimizer' component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows
OID:1.3.6.1.4.1.25623.1.0.812646
Version used: 2022-07-20T10:33:02Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2018-2668
cve: CVE-2018-2665
cve: CVE-2018-2622
cve: CVE-2018-2640
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0424
dfn-cert: DFN-CERT-2018-0286
dfn-cert: DFN-CERT-2018-0101

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (cpuoct2020) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.50
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.50, 5.7.32, 8.0.22 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.49 and prior, 5.7 through 5.7.31 and 8.0 through 8.0.21.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.108959
Version used: 2021-08-16T12:00:57Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**

cve: CVE-2020-14765
cve: CVE-2020-14769
cve: CVE-2020-14812
cve: CVE-2020-14793
cve: CVE-2020-14672
cve: CVE-2020-14867
url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL
advisory-id: cpuoct2020
cert-bund: CB-K20/1066
cert-bund: CB-K20/1017
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2763
dfn-cert: DFN-CERT-2020-2756
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2380
dfn-cert: DFN-CERT-2020-2295

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (cpuoct2019) - Windows

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

Installed version: 5.5.20
Fixed version: 5.6.46
Installation
path / port: 3306/tcp

**Solution:**

**Solution type:** VendorFix
Update to version 5.6.46, 5.7.28, 8.0.18 or later.

**Affected Software/OS**

Oracle MySQL Server versions 5.6.45 and prior, 5.7 through 5.7.27 and 8.0 through 8.0.17.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143030
Version used: `2021-09-07T14:01:38Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2019-2974`
`cve: CVE-2019-2911`
`url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL`
`advisory-id: cpuoct2019`
`cert-bund: CB-K20/1030`
`cert-bund: CB-K20/0109`
`cert-bund: CB-K19/0915`
`dfn-cert: DFN-CERT-2020-2763`
`dfn-cert: DFN-CERT-2020-2756`
`dfn-cert: DFN-CERT-2020-2620`
`dfn-cert: DFN-CERT-2020-2299`
`dfn-cert: DFN-CERT-2020-2180`
`dfn-cert: DFN-CERT-2020-1827`
`dfn-cert: DFN-CERT-2020-0658`
`dfn-cert: DFN-CERT-2020-0517`
`dfn-cert: DFN-CERT-2020-0103`
`dfn-cert: DFN-CERT-2019-2695`
`dfn-cert: DFN-CERT-2019-2687`
`dfn-cert: DFN-CERT-2019-2656`
`dfn-cert: DFN-CERT-2019-2301`
`dfn-cert: DFN-CERT-2019-2149`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

**Summary**
Oracle MySQL Server is prone to an unspecified denial of service vulnerability.

**Vulnerability Detection Result**
```
Installed version: 5.5.20
Fixed version:     5.6.47
Installation
path / port:       3306/tcp
```

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.47 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.46 and prior.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows`
OID:1.3.6.1.4.1.25623.1.0.143359
Version used: `2021-08-16T09:00:57Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
```
cve: CVE-2020-2579
url: https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL
advisory-id: cpujan2020
cert-bund: CB-K20/0038
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0096
```

## Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)

**Product detection result**
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

... continues on next page ...

... continued from previous page ...

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.36 and earlier and 5.6.16 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Performance Schema, Options, RBR.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804575
Version used: `2022-07-21T10:11:30Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-2430`
`cve: CVE-2014-2431`
`cve: CVE-2014-2436`
`cve: CVE-2014-2440`
`url: http://secunia.com/advisories/57940`
`url: http://www.securityfocus.com/bid/66850`
`url: http://www.securityfocus.com/bid/66858`
`url: http://www.securityfocus.com/bid/66890`
`url: http://www.securityfocus.com/bid/66896`
`url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638`

... continues on next page ...

... continued from previous page ...

```
url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0464
cert-bund: CB-K14/0452
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0477
dfn-cert: DFN-CERT-2014-0459
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (cpujul2016) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**

**Solution type:** VendorFix

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

**Affected Software/OS**

Oracle MySQL Server versions 5.5.49 and prior, 5.6 through 5.6.30 and 5.7 through 5.7.12.

**Vulnerability Insight**

Multiple unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**

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

Details: `Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (. ↪..`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.808588
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-3477
cve: CVE-2016-3521
cve: CVE-2016-3615
cve: CVE-2016-5440
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91902
url: http://www.securityfocus.com/bid/91932
url: http://www.securityfocus.com/bid/91960
url: http://www.securityfocus.com/bid/91953
advisory-id: cpujul2016
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1448
cert-bund: CB-K16/1146
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1540
dfn-cert: DFN-CERT-2016-1217
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (cpuoct2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

**Impact**
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.50 and prior, 5.6 through 5.6.31 and 5.7 through 5.7.13.

**Vulnerability Insight**
The flaw exists due to an unspecified error in the 'Server: DML' component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809374
Version used: `2022-07-21T10:11:30Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

```
cve: CVE-2016-5612
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K16/1979
cert-bund: CB-K16/1755
cert-bund: CB-K16/1742
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2016-2089
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.51 and prior.

**Vulnerability Insight**
The flaw exists due to an unspecified error within the 'Server:DML' component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809378
Version used: 2022-07-21T10:11:30Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-5624
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL

... continues on next page ...

... continued from previous page ...

```
advisory-id: cpuoct2016
cert-bund: CB-K16/1846
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714
```

Medium (CVSS: 6.4)
NVT: Oracle MySQL Server Multiple Vulnerabilities-04 Nov12 (Windows)

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

**Impact**

Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data, and cause a DoS (Denial of Service).

**Solution:**

**Solution type:** VendorFix

Apply the patch from the referenced vendor advisory or upgrade to the latest version.

**Affected Software/OS**

Oracle MySQL version 5.5.x to 5.5.26 on Windows.

**Vulnerability Insight**

The flaws are due to multiple unspecified errors in MySQL server component vectors related to MySQL client and server.

**Vulnerability Detection Method**

Details: `Oracle MySQL Server Multiple Vulnerabilities-04 Nov12 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803114
Version used: `2022-04-27T12:01:52Z`

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-3147
cve: CVE-2012-3149
cve: CVE-2012-3144
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56006
url: http://www.securityfocus.com/bid/56008
url: http://www.securityfocus.com/bid/56022
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937

## Medium (CVSS: 6.2)
## NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpuoct2019) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a local unauthenticated vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.45
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.45, 5.7.27, 8.0.17 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143032
Version used: `2021-09-08T08:01:40Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2019-2969`
`url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL`
`advisory-id: cpuoct2019`
`cert-bund: CB-K19/0915`
`dfn-cert: DFN-CERT-2019-2149`

## Medium (CVSS: 6.1)
## NVT: Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (cpuapr2016v3) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.47 and prior, 5.6 through 5.6.28 and 5.7 through 5.7.10.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.47 / 5.6 <= 5.6.28 / 5.7 <= 5.7.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807928
Version used: `2021-10-13T11:01:26Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2016-0649`
`cve: CVE-2016-0650`
`cve: CVE-2016-0644`
`cve: CVE-2016-0646`
`cve: CVE-2016-0640`
`cve: CVE-2016-0641`
`url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL`
`advisory-id: cpuapr2016v3`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0750`
`cert-bund: CB-K16/0646`
`cert-bund: CB-K16/0597`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0903`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0803`
`dfn-cert: DFN-CERT-2016-0695`
`dfn-cert: DFN-CERT-2016-0644`

Medium (CVSS: 5.9)
NVT: Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

**Solution:**
**Solution type:** VendorFix
Apply the latest patch from vendor. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL version 5.5.59 and earlier, 5.6.39 and earlier, 5.7.21 and earlier on Windows

**Vulnerability Insight**
Multiple flaws exist due to
- Multiple errors in the 'Client programs' component of MySQL Server.
- An error in the 'Server: Locking' component of MySQL Server.
- An error in the 'Server: Optimizer' component of MySQL Server.
- Multiple errors in the 'Server: DDL' component of MySQL Server.
- Multiple errors in the 'Server: Replication' component of MySQL Server.
- An error in the 'InnoDB' component of MySQL Server.
- An error in the 'Server : Security : Privileges' component of MySQL Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.813148
Version used: 2022-08-08T10:24:51Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log

. . . continues on next page . . .

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-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: CB-K18/0608
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0913
dfn-cert: DFN-CERT-2018-0723

Medium (CVSS: 5.9)
NVT: Oracle MySQL Backronym Vulnerability June16 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to the backronym vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.3
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack.

**Solution:**
**Solution type:** VendorFix
Upgrade to version Oracle MySQL Server 5.7.3 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL Server 5.7.2 and earlier on Windows.

**Vulnerability Insight**
The flaw exists due to improper validation of MySQL client library when establishing a secure connection to a MySQL server using the –ssl option.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Backronym Vulnerability June16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808063
Version used: `2022-08-08T10:24:51Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2015-3152`
`url: http://www.ocert.org/advisories/ocert-2015-003.html`
`url: https://duo.com/blog/backronym-mysql-vulnerability`
`cert-bund: CB-K18/0871`
`cert-bund: CB-K16/0944`
`cert-bund: CB-K15/1045`
`cert-bund: CB-K15/1042`
`cert-bund: CB-K15/1020`
`cert-bund: CB-K15/0994`
`cert-bund: CB-K15/0964`
`cert-bund: CB-K15/0895`
`dfn-cert: DFN-CERT-2016-1004`
`dfn-cert: DFN-CERT-2015-1105`
`dfn-cert: DFN-CERT-2015-1096`
`dfn-cert: DFN-CERT-2015-1071`
`dfn-cert: DFN-CERT-2015-1051`
`dfn-cert: DFN-CERT-2015-1016`
`dfn-cert: DFN-CERT-2015-0942`

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a vulnerability in a third party library.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
The flaw makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.45 and prior and 5.6 through 5.6.26.

**Vulnerability Insight**
wolfSSL (formerly CyaSSL) as used in MySQL does not properly handle faults associated with the Chinese Remainder Theorem (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117194
Version used: 2022-08-31T10:10:28Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-7744
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
advisory-id: cpujan2016
cert-bund: CB-K16/0246

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0245
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0104

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpuapr2019) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.43
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.43, 5.7.25, 8.0.14 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.42 and prior, 5.7 through 5.7.24 and 8.0 through 8.0.13.

**Vulnerability Insight**
Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.142405
Version used: 2021-09-07T14:01:38Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2018-3123
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
advisory-id: cpuapr2019
cert-bund: CB-K19/0319
dfn-cert: DFN-CERT-2019-0775

## Medium (CVSS: 5.9)
## NVT: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (cpuapr2019) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.44
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.44, 5.7.26, 8.0.16 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.43 and prior, 5.7 through 5.7.25 and 8.0 through 8.0.15.

**Vulnerability Insight**
The attacks range in variety and difficulty. Most of them allow an attacker with network access via multiple protocols to compromise the MySQL Server.
For further information refer to the official advisory via the referenced link.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (.

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.142403
Version used: 2022-03-28T03:06:01Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2019-1559
cve: CVE-2019-2683
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-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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0968
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.7.33
Installation
path / port:       3306/tcp
```

**Solution:**

**Solution type:** VendorFix

Update to version 5.7.33, 8.0.23 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL Server version 5.7.32 and prior and 8.0 through 8.0.22.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145794
Version used: `2021-08-26T13:01:12Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2020-1971`
`cve: CVE-2021-2178`
`cve: CVE-2021-2202`
`url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL`
`advisory-id: cpuapr2021`
`cert-bund: WID-SEC-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`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2021-0255
dfn-cert: DFN-CERT-2021-0134
dfn-cert: DFN-CERT-2021-0131
dfn-cert: DFN-CERT-2021-0128
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2021-0078
dfn-cert: DFN-CERT-2021-0012
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668
```

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.7.35
Installation
path / port:       3306/tcp
```

**Solution:**

**Solution type:** VendorFix

Update to version 5.7.35, 8.0.26 or later.

**Affected Software/OS**

Oracle MySQL Server version 5.7.34 and prior and 8.0 through 8.0.25.

**Vulnerability Detection Method**

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

Details: `Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Wi.
↪..`

OID:1.3.6.1.4.1.25623.1.0.146355

... continues on next page ...

... continued from previous page ...

Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-22901
cve: CVE-2019-17543
cve: CVE-2021-2389
cve: CVE-2021-2390
cve: CVE-2021-2356
cve: CVE-2021-2385
cve: CVE-2021-2342
cve: CVE-2021-2372
cve: CVE-2021-22897
cve: CVE-2021-22898
url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL
advisory-id: cpujul2021
cert-bund: WID-SEC-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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-1157
dfn-cert: DFN-CERT-2021-1151
dfn-cert: DFN-CERT-2021-1148
dfn-cert: DFN-CERT-2021-1045
dfn-cert: DFN-CERT-2019-2216

Medium (CVSS: 5.7)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Server : Optimizer, DDL, Server : Compiling, Server : Federated.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805172
Version used: 2022-04-14T06:42:08Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-2571
cve: CVE-2015-0505
cve: CVE-2015-0501
cve: CVE-2015-0499
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74095
url: http://www.securityfocus.com/bid/74112
url: http://www.securityfocus.com/bid/74070
url: http://www.securityfocus.com/bid/74115
cert-bund: CB-K15/1546
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551

Medium (CVSS: 5.6)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow remote to have an impact on availability, confidentiality and integrity.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.53 and earlier, 5.6.34 and earlier, 5.7.16 and earlier on Windows

**Vulnerability Insight**
Multiple flaws exist due to: multiple unspecified errors in sub components 'Error Handling', 'Logging', 'MyISAM', 'Packaging', 'Optimizer', 'DML' and 'DDL'.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows
OID:1.3.6.1.4.1.25623.1.0.809865
Version used: 2022-08-03T10:11:15Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-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: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95571

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/95560
url: http://www.securityfocus.com/bid/95491
url: http://www.securityfocus.com/bid/95527
url: http://www.securityfocus.com/bid/95565
url: http://www.securityfocus.com/bid/95588
url: http://www.securityfocus.com/bid/95501
url: http://www.securityfocus.com/bid/95585
url: http://www.securityfocus.com/bid/95520
cert-bund: CB-K18/0224
cert-bund: CB-K17/1732
cert-bund: CB-K17/1604
cert-bund: CB-K17/1298
cert-bund: CB-K17/0927
cert-bund: CB-K17/0423
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0959
dfn-cert: DFN-CERT-2017-0430
dfn-cert: DFN-CERT-2017-0090
```

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.7.37
Installation
path / port:       3306/tcp
```

**Solution:**

**Solution type:** VendorFix

Update to version 5.7.37, 8.0.28 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.147465
Version used: `2022-01-26T03:03:43Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2021-22946`
`cve: CVE-2022-21367`
`cve: CVE-2022-21270`
`cve: CVE-2022-21304`
`cve: CVE-2022-21344`
`cve: CVE-2022-21303`
`cve: CVE-2022-21245`
`cve: CVE-2021-22947`
`url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL`
`advisory-id: cpujan2022`
`cert-bund: WID-SEC-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`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0052
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-1931
```

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     See the referenced vendor advisory
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow local users to affect availability.

**Solution:**

**Solution type:** VendorFix

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

**Affected Software/OS**

Oracle MySQL Server versions 5.5.46 and prior.

**Vulnerability Insight**

Unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Optimizer'.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows
OID:1.3.6.1.4.1.25623.1.0.807922
Version used: 2022-08-31T10:10:28Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-0651
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0597
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0644

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (cpujul2019) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.45
Installation
path / port: 3306/tcp

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

... continues on next page ...

... continued from previous page ...

Update to version 5.6.45, 5.7.27, 8.0.17 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

**Vulnerability Insight**
Oracle MySQL Server is prone to multiple denial of service vulnerabilities.
For further information refer to the official advisory via the referenced link.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.. ↪..`
OID:1.3.6.1.4.1.25623.1.0.142645
Version used: `2021-09-07T14:01:38Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2019-2805`
`cve: CVE-2019-2740`
`cve: CVE-2019-2819`
`cve: CVE-2019-2739`
`cve: CVE-2019-2737`
`cve: CVE-2019-2738`
`url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL`
`advisory-id: cpujul2019`
`cert-bund: CB-K19/0620`
`dfn-cert: DFN-CERT-2020-2620`
`dfn-cert: DFN-CERT-2020-2180`
`dfn-cert: DFN-CERT-2020-0658`
`dfn-cert: DFN-CERT-2020-0517`
`dfn-cert: DFN-CERT-2019-2695`
`dfn-cert: DFN-CERT-2019-2656`
`dfn-cert: DFN-CERT-2019-2300`
`dfn-cert: DFN-CERT-2019-2008`
`dfn-cert: DFN-CERT-2019-1713`
`dfn-cert: DFN-CERT-2019-1683`
`dfn-cert: DFN-CERT-2019-1568`
`dfn-cert: DFN-CERT-2019-1453`

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.40, 8.0.31 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.30.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118388
Version used: 2022-10-24T10:14:58Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2022-2097
cve: CVE-2022-21617
cve: CVE-2022-21608
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1777
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1461

... continues on next page ...

... continued from previous page ...

```
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-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 (apr2017-3236618) 03 - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to a security bypass vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation of this vulnerability will allow remote attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack. This may lead to other attacks also.

**Solution:**

**Solution type:** VendorFix

Apply the patch from the referenced advisory.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier on Windows

**Vulnerability Insight**
The flaw exists due to an incorrect implementation or enforcement of 'ssl-mode=REQUIRED' in MySQL.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810884
Version used: `2022-04-13T11:57:07Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2017-3305`
`url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html`
`url: http://www.securityfocus.com/bid/97023`
`cert-bund: CB-K17/1604`
`cert-bund: CB-K17/1239`
`cert-bund: CB-K17/0657`
`dfn-cert: DFN-CERT-2017-1675`
`dfn-cert: DFN-CERT-2017-1282`
`dfn-cert: DFN-CERT-2017-0675`

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version: 5.6.46`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.46, 5.7.28 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.45 and prior and 5.7 through 5.7.27.

**Vulnerability Insight**
Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 Security Update (cpuoct2019) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.143034
Version used: 2021-09-08T08:01:40Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2019-2922
cve: CVE-2019-2923
cve: CVE-2019-2924
cve: CVE-2019-2910
url: https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
advisory-id: cpuoct2019
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2019-2149

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**Summary**
Oracle MySQL is prone to vulnerability.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version: Apply the patch`

**Impact**
Successful exploitation of this vulnerability will allow remote attackers to partially access data, partially modify data, and partially deny service.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, on Windows

**Vulnerability Insight**
The flaw exists due to an error in the Client programs component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811434
Version used: `2022-08-08T10:24:51Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2017-3636`
`url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html`
`↪#AppendixMSQL`
`url: http://www.securityfocus.com/bid/99736`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/1870`
`cert-bund: CB-K17/1604`
`cert-bund: CB-K17/1453`
`cert-bund: CB-K17/1401`
`cert-bund: CB-K17/1239`
`cert-bund: CB-K17/1205`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.47
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.47, 5.7.27 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.46 and prior and 5.7 through 5.7.26.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.143735
Version used: 2021-08-16T09:00:57Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**

cve: CVE-2019-1547
cve: CVE-2019-1549
cve: CVE-2019-1552
cve: CVE-2019-1563
url: https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL
advisory-id: cpuapr2020
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/1016
cert-bund: CB-K20/0321
cert-bund: CB-K20/0318
cert-bund: CB-K20/0043
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
cert-bund: CB-K20/0028
cert-bund: CB-K19/1025
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0808
cert-bund: CB-K19/0675
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1900
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1559

Medium (CVSS: 5.0)
NVT: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

**Summary**
MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL 5.5.30 and earlier and 5.6.10 on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Prepared Statements, Server Options and Server Partition.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803725
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-3801
cve: CVE-2013-3805
cve: CVE-2013-3794
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61222
url: http://www.securityfocus.com/bid/61256
url: http://www.securityfocus.com/bid/61269
cert-bund: CB-K13/0919
cert-bund: CB-K13/0620

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 5.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier on windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to DDL, Server : Security : Privileges, Server : Security : Encryption, InnoDB : DML.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805171
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log

... continues on next page ...

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

cve: CVE-2015-2573
cve: CVE-2015-2568
cve: CVE-2015-0441
cve: CVE-2015-0433
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74078
url: http://www.securityfocus.com/bid/74073
url: http://www.securityfocus.com/bid/74103
url: http://www.securityfocus.com/bid/74089
cert-bund: CB-K15/1546
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**

Installed version: 5.5.20
Fixed version: 5.7.34
Installation

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.34 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.33 and prior.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows
OID:1.3.6.1.4.1.25623.1.0.145802
Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-2154
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2021-1660
dfn-cert: DFN-CERT-2021-0984
dfn-cert: DFN-CERT-2021-0821

## Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpujan2021) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.51
Installation
path / port: 3306/tcp

**Impact**
Successful attacks of this vulnerability can result in the unauthorized ability to cause a hang or frequently repeatedly crash (complete DOS) the MySQL Server.

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.51, 5.7.31, 8.0.18 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.30 and 8.0 through 8.0.17.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.145222
Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-2001
url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL
advisory-id: cpujan2021
cert-bund: CB-K21/0062
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0810
dfn-cert: DFN-CERT-2021-0131

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpujan2021) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log

... continues on next page ...

... continued from previous page ...

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

**Summary**
Oracle MySQL Server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.6.51
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.51, 5.7.33, 8.0.23 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.32 and 8.0 through 8.0.22.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.145224
Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-2022
cve: CVE-2021-2060
url: https://www.oracle.com/security-alerts/cpujan2021.html#AppendixMSQL
advisory-id: cpujan2021
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 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Windows

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.31
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.31, 8.0.18 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.30 and prior and 8.0 through 8.0.17.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145804
Version used: 2021-08-26T13:01:12Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2021-2160
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2021-0821

Medium (CVSS: 4.9)
NVT: Oracle MySQL Security Update (cpujul2018 - 04) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log

... continues on next page ...

... continued from previous page ...

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

**Summary**
Oracle MySQL is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

**Solution:**
**Solution type:** VendorFix
The vendor has released updates. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL version 5.5.60 and earlier.

**Vulnerability Insight**
Multiple flaws exist due to an error in the 'Server: Security: Privileges' component of MySQL Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Security Update (cpujul2018 - 04) - Windows
OID:1.3.6.1.4.1.25623.1.0.813710
Version used: 2022-08-22T10:11:10Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2018-3063
url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL
advisory-id: cpujul2018
cert-bund: CB-K18/0795
dfn-cert: DFN-CERT-2019-1614

... continues on next page ...

... continued from previous page ...

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)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to an unspecified vulnerability.

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

**Impact**
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows

**Vulnerability Insight**
Unspecified error in the MySQL Server component via unknown vectors related to Replication.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 .
↪..
OID:1.3.6.1.4.1.25623.1.0.804034
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-5807
url: http://secunia.com/advisories/55327
url: http://www.securityfocus.com/bid/63105
url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
cert-bund: CB-K14/0187
cert-bund: CB-K13/1072
cert-bund: CB-K13/0840
cert-bund: CB-K13/0789
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1846
dfn-cert: DFN-CERT-2013-1795

Medium (CVSS: 4.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807924
Version used: `2022-08-31T10:10:28Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2016-0666`
`cve: CVE-2016-0647`
`cve: CVE-2016-0648`
`cve: CVE-2016-0642`
`cve: CVE-2016-0643`
`cve: CVE-2016-2047`
`url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL`
`advisory-id: cpuapr2016v3`
`cert-bund: CB-K16/1129`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0750`
`cert-bund: CB-K16/0646`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0493`
`cert-bund: CB-K16/0133`
`dfn-cert: DFN-CERT-2016-1204`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0903`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0803`
`dfn-cert: DFN-CERT-2016-0695`
`dfn-cert: DFN-CERT-2016-0644`
`dfn-cert: DFN-CERT-2016-0532`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0143

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.40, 8.0.17 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.16.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.16 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118384
Version used: 2022-10-24T10:14:58Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2022-21589
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.40, 8.0.30 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.29.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.29 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118386
Version used: 2022-10-24T10:14:58Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2022-21592
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.5.30, 5.6.11 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.5 through 5.5.29 and 5.6 through 5.6.10.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.29 / 5.6 <= 5.6.11 Security Update (cpuapr2013) .
↪..
OID:1.3.6.1.4.1.25623.1.0.117213
Version used: 2021-02-12T11:09:59Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-1523
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to a denial of service (DoS) vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.7.37
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.7.37, 8.0.28 or later.

**Affected Software/OS**
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118382
Version used: 2022-10-24T10:14:58Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2022-21595
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2022-1776
dfn-cert: DFN-CERT-2022-2306

Medium (CVSS: 4.4)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.53 and earlier on Windows

**Vulnerability Insight**
The flaw exists due to an unspecified error in sub component 'Server: Charsets'.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.809869
Version used: 2022-10-31T10:12:00Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2017-3243
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html

. . . continues on next page . . .

... continued from previous page ...

url: http://www.securityfocus.com/bid/95538
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0090

Medium (CVSS: 4.3)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier on Windows

**Vulnerability Insight**
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server : Pluggable Auth and Server : Security : Privileges.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15
OID:1.3.6.1.4.1.25623.1.0.805930

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-4737
cve: CVE-2015-2620
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75802
url: http://www.securityfocus.com/bid/75837
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071

Medium (CVSS: 4.2)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch

**Impact**
Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availablility.

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

... continues on next page ...

... continued from previous page ...

Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, 5.7.18 and earlier, on Windows

**Vulnerability Insight**
Multiple flaws exist due to
- A flaw in the Client mysqldump component.
- A flaw in the Server: DDL component.
- A flaw in the C API component.
- A flaw in the Connector/C component.
- A flaw in the Server: Charsets component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811432
Version used: `2022-04-13T11:57:07Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2017-3651`
`cve: CVE-2017-3653`
`cve: CVE-2017-3652`
`cve: CVE-2017-3635`
`cve: CVE-2017-3648`
`cve: CVE-2017-3641`
`url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html`
`↪#AppendixMSQL`
`url: http://www.securityfocus.com/bid/99802`
`url: http://www.securityfocus.com/bid/99810`
`url: http://www.securityfocus.com/bid/99805`
`url: http://www.securityfocus.com/bid/99730`
`url: http://www.securityfocus.com/bid/99789`
`url: http://www.securityfocus.com/bid/99767`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/1870`
`cert-bund: CB-K17/1732`
`cert-bund: CB-K17/1604`
`cert-bund: CB-K17/1453`
`cert-bund: CB-K17/1401`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1298
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1806
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243

Medium (CVSS: 4.0)
NVT: MySQL Server Component Partition Unspecified Vulnerability

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
MySQL is prone to an unspecified vulnerability.

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

**Impact**
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
MySQL version 5.5.x before 5.5.22

**Vulnerability Insight**
Unspecified error in MySQL Server component related to Partition.

**Vulnerability Detection Method**
Details: MySQL Server Component Partition Unspecified Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.803801
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-1697
url: http://secunia.com/advisories/48890
url: http://www.securityfocus.com/bid/53064
url: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#Ap
↪pendixMSQL
dfn-cert: DFN-CERT-2012-0939
dfn-cert: DFN-CERT-2012-0735

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities-03 Nov12 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL server is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch

**Impact**
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced vendor advisory or upgrade to latest version.

**Affected Software/OS**
Oracle MySQL version 5.1.x to 5.1.63 and Oracle MySQL version 5.5.x to 5.5.25 on Windows.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The flaws are due to multiple unspecified errors in MySQL server component vectors related to InnoDB plugin, server full text search and InnoDB.

**Vulnerability Detection Method**
Details: Oracle MySQL Server Multiple Vulnerabilities-03 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803113
Version used: 2022-04-27T12:01:52Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-3173
cve: CVE-2012-3167
cve: CVE-2012-3166
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56018
url: http://www.securityfocus.com/bid/56028
url: http://www.securityfocus.com/bid/56041
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.46 and prior.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.46 Security Update (cpujan2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117190
Version used: `2021-02-12T11:09:59Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2016-0616`
`url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL`
`advisory-id: cpujan2016`
`cert-bund: CB-K16/1122`
`cert-bund: CB-K16/0936`
`cert-bund: CB-K16/0791`
`cert-bund: CB-K16/0493`
`cert-bund: CB-K16/0246`
`cert-bund: CB-K16/0245`
`cert-bund: CB-K16/0133`
`cert-bund: CB-K16/0094`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-0994`
`dfn-cert: DFN-CERT-2016-0845`
`dfn-cert: DFN-CERT-2016-0532`
`dfn-cert: DFN-CERT-2016-0266`
`dfn-cert: DFN-CERT-2016-0265`
`dfn-cert: DFN-CERT-2016-0143`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0104

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.46 and prior and 5.6 through 5.6.27.

**Vulnerability Insight**
Unspecified errors exist in the 'MySQL Server' component via unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.806877
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**

```
cve: CVE-2016-0596
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81176
url: http://www.securityfocus.com/bid/81198
url: http://www.securityfocus.com/bid/81130
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0143
dfn-cert: DFN-CERT-2016-0104
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to disclose potentially sensitive information, gain escalated privileges, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

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

**Affected Software/OS**
Oracle MySQL Server versions 5.5.38 and prior.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to SERVER:DDL.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804783
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-6520`
`url: https://www.oracle.com/security-alerts/cpuoct2014.html#AppendixMSQL`
`url: http://www.securityfocus.com/bid/70510`
`advisory-id: cpuoct2014`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K15/0415`
`cert-bund: CB-K14/1482`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/1412`
`cert-bund: CB-K14/1299`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2015-0427`
`dfn-cert: DFN-CERT-2014-1567`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-1489`
`dfn-cert: DFN-CERT-2014-1357`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.24
Installation
path / port: 3306/tcp

**Impact**
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'GIS Extension' package / privilege.

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.63, 5.5.24 or later.

**Affected Software/OS**
Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.23.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - .
↪..
OID:1.3.6.1.4.1.25623.1.0.117265
Version used: 2021-03-18T11:53:07Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-0540
cve: CVE-2012-1734
cve: CVE-2012-2749

... continues on next page ...

... continued from previous page ...

```
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

| | |
|---|---|
| Installed version: | 5.5.20 |
| Fixed version: | 5.5.23 |
| Installation path / port: | 3306/tcp |

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

**Solution:**
**Solution type:** VendorFix
Update to version 5.1.63, 5.5.23 or later.

**Affected Software/OS**
Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.22 Security Update (cpujul2012) - ...`
OID:1.3.6.1.4.1.25623.1.0.117263
Version used: `2021-03-18T11:53:07Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`

... continues on next page ...

... continued from previous page ...

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2012-1689
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389

## Medium (CVSS: 4.0)
## NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Update to version 5.5.31, 5.6.11 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.10.

**Vulnerability Insight**
Unspecified error in some unknown vectors related to Stored Procedure.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) .
↪..
OID:1.3.6.1.4.1.25623.1.0.809815
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-2376
cve: CVE-2013-1511
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59227
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

**Solution:**
**Solution type:** VendorFix
Update to version 5.5.30 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.5 through 5.5.29.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows`
OID:1.3.6.1.4.1.25623.1.0.117215
Version used: `2021-02-12T11:09:59Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-1512`
`cve: CVE-2013-1526`
`url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL`
`advisory-id: cpuapr2013`
`dfn-cert: DFN-CERT-2013-0798`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
`Installed version: 5.5.20`

**Impact**
Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to DLL.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805135
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

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

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 July14 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20-log
Vulnerable range: 5.5 - 5.5.37

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.37 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to ENARC and SROPTZR.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 July14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804723
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-2494`
`cve: CVE-2014-4207`
`url: http://secunia.com/advisories/59521`
`url: http://www.securityfocus.com/bid/68579`
`url: http://www.securityfocus.com/bid/68593`
`url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi`
`↪ty_patches`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A`
`↪ppendixMSQL`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/0891`
`cert-bund: CB-K14/0868`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-0930`
`dfn-cert: DFN-CERT-2014-0911`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20

**Impact**
Successful exploitation will allow attackers to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server version 5.5.40 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Server:InnoDB:DDL:Foreign Key

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805133
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-0432
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72217
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

**Solution:**

**Solution type:** VendorFix

Apply the patch from the referenced advisory.

**Affected Software/OS**

Oracle MySQL Server 5.5.44 and earlier on windows

**Vulnerability Insight**

Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

**Vulnerability Detection Method**

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

... continues on next page ...

... continued from previous page ...

Details: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805771
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-4816
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77134
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 Jul15

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow an authenticated remote attacker to cause denial-of-service attack.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors exist in the MySQL Server component via unknown vectors related to DML, Server : I_S, Server : Optimizer, and GIS.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-02 Jul15`
OID:1.3.6.1.4.1.25623.1.0.805929
Version used: `2022-04-14T06:42:08Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2015-2648`
`cve: CVE-2015-4752`
`cve: CVE-2015-2643`
`cve: CVE-2015-2582`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html`
`url: http://www.securityfocus.com/bid/75822`
`url: http://www.securityfocus.com/bid/75849`
`url: http://www.securityfocus.com/bid/75830`
`url: http://www.securityfocus.com/bid/75751`
`cert-bund: CB-K15/1202`
`cert-bund: CB-K15/1193`
`cert-bund: CB-K15/1045`
`cert-bund: CB-K15/1020`
`dfn-cert: DFN-CERT-2015-1272`
`dfn-cert: DFN-CERT-2015-1264`
`dfn-cert: DFN-CERT-2015-1096`
`dfn-cert: DFN-CERT-2015-1071`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to affect confidentiality, integrity, and availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier on windows

**Vulnerability Insight**
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805764
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2015-4913
cve: CVE-2015-4830

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2015-4826
cve: CVE-2015-4815
cve: CVE-2015-4807
cve: CVE-2015-4802
cve: CVE-2015-4792
cve: CVE-2015-4870
cve: CVE-2015-4861
cve: CVE-2015-4858
cve: CVE-2015-4836
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
url: http://www.securityfocus.com/bid/77153
url: http://www.securityfocus.com/bid/77228
url: http://www.securityfocus.com/bid/77237
url: http://www.securityfocus.com/bid/77222
url: http://www.securityfocus.com/bid/77205
url: http://www.securityfocus.com/bid/77165
url: http://www.securityfocus.com/bid/77171
url: http://www.securityfocus.com/bid/77208
url: http://www.securityfocus.com/bid/77137
url: http://www.securityfocus.com/bid/77145
url: http://www.securityfocus.com/bid/77190
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-06 July-2013 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**Summary**
MySQL is prone to an unspecified vulnerability.

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

**Impact**
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL 5.5.31 and earlier on Windows.

**Vulnerability Insight**
Unspecified error in the MySQL Server component via unknown vectors related to Server Parser.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerability-06 July-2013 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803728
Version used: `2022-04-25T14:50:49Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-3783`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61210`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerability-04 July-2013 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
MySQL is prone to an unspecified vulnerability.

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

**Impact**
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier and 5.6.10 on Windows.

**Vulnerability Insight**
Unspecified error in the MySQL Server component via unknown vectors related to Server Options.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerability-04 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803726
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-3808
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61227
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-1599

. . . continues on next page . . .

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Optimizer, InnoDB, and Locking.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804076
Version used: 2022-04-14T11:24:11Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**

cve: CVE-2014-0386
cve: CVE-2014-0393
cve: CVE-2014-0402
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64877
url: http://www.securityfocus.com/bid/64904
url: http://www.securityfocus.com/bid/64908
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0177
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0180
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 04 Jan14 (Windows)

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

Oracle MySQL is prone to multiple unspecified vulnerabilities.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

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 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to InnoDB, Optimizer, Error Handling, and some unknown vectors.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 04 Jan14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804075
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2014-0401`
`cve: CVE-2014-0412`
`cve: CVE-2014-0437`
`cve: CVE-2013-5908`
`url: http://secunia.com/advisories/56491`
`url: http://www.securityfocus.com/bid/64849`
`url: http://www.securityfocus.com/bid/64880`
`url: http://www.securityfocus.com/bid/64896`
`url: http://www.securityfocus.com/bid/64898`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html`
`cert-bund: CB-K15/1518`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K14/0177`
`cert-bund: CB-K14/0082`
`cert-bund: CB-K14/0074`
`cert-bund: CB-K14/0055`
`dfn-cert: DFN-CERT-2015-1604`
`dfn-cert: DFN-CERT-2014-0742`
`dfn-cert: DFN-CERT-2014-0190`
`dfn-cert: DFN-CERT-2014-0180`
`dfn-cert: DFN-CERT-2014-0085`
`dfn-cert: DFN-CERT-2014-0074`
`dfn-cert: DFN-CERT-2014-0048`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.33 and earlier on Windows, Oracle MySQL version 5.6.13 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Partition.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804074
Version used: `2022-04-14T11:24:11Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-5891`
`url: http://secunia.com/advisories/56491`
`url: http://www.securityfocus.com/bid/64891`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html`

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.35 and earlier and 5.6.15 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Partition, Replication and XML subcomponent.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804574

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-14T11:24:11Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2014-0384
cve: CVE-2014-2419
cve: CVE-2014-2438
url: http://secunia.com/advisories/57940
url: http://www.securityfocus.com/bid/66835
url: http://www.securityfocus.com/bid/66846
url: http://www.securityfocus.com/bid/66880
url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638
url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0464
cert-bund: CB-K14/0452
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0477
dfn-cert: DFN-CERT-2014-0459

## Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability Oct-2013 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to an unspecified vulnerability.

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

**Impact**
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

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

... continues on next page ...

... continued from previous page ...

Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL versions 5.1.51 through 5.1.70, 5.5.10 through 5.5.32, and 5.6.x through 5.6.12 on Windows.

**Vulnerability Insight**
Unspecified error in the MySQL Server component via unknown vectors related to Optimizer.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability Oct-2013 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.804033
Version used: `2022-04-25T14:50:49Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-3839`
`url: http://secunia.com/advisories/55327`
`url: http://www.securityfocus.com/bid/63109`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0840`
`cert-bund: CB-K13/0806`
`cert-bund: CB-K13/0789`
`dfn-cert: DFN-CERT-2014-0190`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1846`
`dfn-cert: DFN-CERT-2013-1815`
`dfn-cert: DFN-CERT-2013-1795`

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-02 July-2013 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

... continues on next page ...

... continued from previous page ...

**Summary**
MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow remote authenticated users to affect integrity and availability via unknown vectors and cause denial of service.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL 5.5.31 and earlier, 5.6.11 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Server Replication, Audit Log and Data Manipulation Language.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MySQL Unspecified vulnerabilities-02 July-2013 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803724
Version used: `2022-04-25T14:50:49Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2013-3812`
`cve: CVE-2013-3809`
`cve: CVE-2013-3793`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61249`
`url: http://www.securityfocus.com/bid/61264`
`url: http://www.securityfocus.com/bid/61272`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: MySQL Unspecified vulnerabilities-01 July-2013 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, 5.6.11 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Full Text Search and Server Optimizer.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-01 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803723
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

... continues on next page ...

... continued from previous page ...

**References**
cve: CVE-2013-3804
cve: CVE-2013-3802
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61244
url: http://www.securityfocus.com/bid/61260
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

[ return to 172.16.1.8 ]

### 2.1.25 Medium 8443/tcp

Medium (CVSS: 5.4)
NVT: SSL/TLS: Report 'Anonymous' Cipher Suites

**Summary**
This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.

**Vulnerability Detection Result**
'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_WITH_AES_128_CBC_SHA

**Impact**
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

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

**Vulnerability Insight**
Services supporting 'Anonymous' cipher suites could allow a client to negotiate an SSL/TLS connection to the host without any authentication of the remote endpoint.

**Vulnerability Detection Method**
Details: SSL/TLS: Report 'Anonymous' Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.108147

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-13T11:57:07Z

**References**

cve: CVE-2007-1858
cve: CVE-2014-0351
url: https://bettercrypto.org/
url: http://www.securityfocus.com/bid/28482
url: http://www.securityfocus.com/bid/69754
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K14/0058
dfn-cert: DFN-CERT-2014-0049
dfn-cert: DFN-CERT-2012-0442

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Vulnerability Detection Result**

The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372

... 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
```

[ return to 172.16.1.8 ]

### 2.1.26 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

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

**Solution:**
**Solution type:** Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

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. This information could theoretically be used to exploit weak time-based random number generators in other services.

**Vulnerability Detection Method**
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

**References**
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[ return to 172.16.1.8 ]

### 2.1.27 Low 9200/tcp

Low (CVSS: 3.1)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)

**Summary**
Elasticsearch is prone to an information disclosure vulnerability.

**Vulnerability Detection Result**
```
Installed version: 1.1.1
Fixed version:     6.8.13
Installation
path / port:       /
```

**Impact**
This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

**Solution:**
**Solution type:** VendorFix
Update to version 6.8.13, 7.9.2 or later.

**Affected Software/OS**
Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
A document disclosure flaw was found in Elasticsearch when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)`
OID:1.3.6.1.4.1.25623.1.0.117181
Version used: `2021-08-17T12:00:57Z`

**References**
```
cve: CVE-2020-7020
url: https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update
↪/253033
url: https://www.elastic.co/community/security
cert-bund: WID-SEC-2022-0607
dfn-cert: DFN-CERT-2022-1530
```

[ return to 172.16.1.8 ]

### 2.1.28 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Vulnerability Detection Result**
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 301229
Packet 2: 301335
```

**Impact**
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution:**
**Solution type:** Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

... continues on next page ...

... continued from previous page ...

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

**Affected Software/OS**
TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

**References**
`url: http://www.ietf.org/rfc/rfc1323.txt`
`url: http://www.ietf.org/rfc/rfc7323.txt`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[ return to 172.16.1.8 ]

### 2.1.29 Low 3306/tcp

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (cpu-jul2016) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version: See the referenced vendor advisory`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

**Impact**
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.10.

**Vulnerability Insight**
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to the 'Security Encryption' sub-component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.808594
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-3452
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91999
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169

## Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpujul2016) - Windows

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: See the referenced vendor advisory
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

**Vulnerability Insight**
An unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Connection' sub-component.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.808593
Version used: 2022-04-13T13:17:10Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2016-5444
url: https://www.oracle.com/security-alerts/cpujul2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/91987
advisory-id: cpujul2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/1100

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-04 Jul15

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
Installed version: 5.5.20
Fixed version: Apply the patch
Installation
path / port: 3306/tcp

**Impact**
Successful exploitation will allow an authenticated remote attacker to cause denial of service attack.

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on Windows.

**Vulnerability Insight**
Unspecified error exists in the MySQL Server component via unknown vectors related to Server : Optimizer.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Unspecified Vulnerability-04 Jul15
OID:1.3.6.1.4.1.25623.1.0.805931
Version used: 2022-04-14T06:42:08Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

```
cve: CVE-2015-4757
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75759
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1020
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1071
```

## Low (CVSS: 3.5)
## NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)

**Product detection result**

```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**

Oracle MySQL is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

```
Installed version: 5.5.20
Fixed version:     Apply the patch
Installation
path / port:       3306/tcp
```

**Impact**

Successful exploitation will allow an authenticated remote attacker to affect integrity via unknown vectors.

**Solution:**

**Solution type:** VendorFix

Apply the patch from the referenced advisory.

**Affected Software/OS**

Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on windows

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805770
Version used: `2022-04-14T06:42:08Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2015-4864`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html`
`url: http://www.securityfocus.com/bid/77187`
`cert-bund: CB-K16/0245`
`cert-bund: CB-K15/1844`
`cert-bund: CB-K15/1554`
`dfn-cert: DFN-CERT-2016-0265`
`dfn-cert: DFN-CERT-2015-1946`
`dfn-cert: DFN-CERT-2015-1638`

## Low (CVSS: 3.5)
NVT: Oracle MySQL Server Multiple Vulnerabilities-05 Nov12 (Windows)

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**
`Installed version: 5.5.20`
`Fixed version:  Apply the patch`

**Impact**
Successful exploitation will allow an attacker to disclose potentially sensitive information and manipulate certain data.

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

... continues on next page ...

... continued from previous page ...

Apply the patch from the linked references or upgrade to latest version.

**Affected Software/OS**
Oracle MySQL version 5.5.x to 5.5.25 on Windows.

**Vulnerability Insight**
The flaw is due to unspecified error in MySQL server component vectors server.

**Vulnerability Detection Method**
Details: `Oracle MySQL Server Multiple Vulnerabilities-05 Nov12 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803115
Version used: `2022-04-27T12:01:52Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2012-3156`
`url: http://secunia.com/advisories/51008/`
`url: http://www.securityfocus.com/bid/56013`
`url: http://www.securelist.com/en/advisories/51008`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html`
`url: https://support.oracle.com/rs?type=doc&id=1475188.1`

Low (CVSS: 3.3)
NVT: Oracle MySQL Security Update (cpujul2018 - 02) - Windows

**Product detection result**
```
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**
```
Installed version: 5.5.20
Fixed version:     See reference
Installation
path / port:       3306/tcp
```

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow remote attackers to have an impact on confidentiality, integrity and availability.

**Solution:**
**Solution type:** VendorFix
The vendor has released updates. Please see the references for more information.

**Affected Software/OS**
Oracle MySQL version 5.5.60 and earlier, 5.6.40 and earlier, 5.7.22 and earlier.

**Vulnerability Insight**
Multiple flaws exist due to errors in 'Server: Security: Encryption', 'Server: Options', 'MyISAM', 'Client mysqldump' components of application.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Security Update (cpujul2018 - 02) - Windows`
OID:1.3.6.1.4.1.25623.1.0.813706
Version used: `2022-08-31T10:10:28Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
`cve: CVE-2018-2767`
`cve: CVE-2018-3066`
`cve: CVE-2018-3058`
`cve: CVE-2018-3070`
`url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL`
`advisory-id: cpujul2018`
`cert-bund: CB-K18/0795`
`dfn-cert: DFN-CERT-2019-1614`
`dfn-cert: DFN-CERT-2019-1588`
`dfn-cert: DFN-CERT-2019-1152`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2019-0484`
`dfn-cert: DFN-CERT-2019-0112`
`dfn-cert: DFN-CERT-2018-1649`
`dfn-cert: DFN-CERT-2018-1402`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-0913`

Low (CVSS: 2.8)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)

**Product detection result**
cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**
Oracle MySQL is prone to multiple unspecified vulnerabilities.

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

**Impact**
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

**Solution:**
**Solution type:** VendorFix
Apply the patch from the referenced advisory.

**Affected Software/OS**
Oracle MySQL version 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

**Vulnerability Insight**
Unspecified errors in the MySQL Server component via unknown vectors related to Replication.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804077
Version used: 2022-04-14T11:24:11Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2014-0420
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64888
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048
```

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Windows

**Product detection result**
`cpe:/a:mysql:mysql:5.5.20-log`
`Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.`
`↪25623.1.0.100152)`

**Summary**
Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

| | |
|---|---|
| Installed version: | 5.5.20 |
| Fixed version: | 5.6.45 |
| Installation path / port: | 3306/tcp |

**Solution:**
**Solution type:** VendorFix
Update to version 5.6.45, 5.7.19 or later.

**Affected Software/OS**
Oracle MySQL Server versions 5.6.44 and prior and 5.7 through 5.7.18.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.142643
Version used: `2021-09-07T14:01:38Z`

**Product Detection Result**
Product: `cpe:/a:mysql:mysql:5.5.20-log`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

cve: CVE-2019-2730
url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
advisory-id: cpujul2019
cert-bund: CB-K19/0620
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-1453

Low (CVSS: 1.5)
NVT: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) - Windows

**Product detection result**

cpe:/a:mysql:mysql:5.5.20-log
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

**Summary**

Oracle MySQL Server is prone to an unspecified vulnerability.

**Vulnerability Detection Result**

Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

**Impact**

Successful exploitation will allow local users to affect availability.

**Solution:**

**Solution type:** VendorFix
Update to version 5.5.31, 5.6.10 or later.

**Affected Software/OS**

Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.9.

**Vulnerability Insight**

An unspecified error exists in the MySQL Server component via unknown vectors related to Server Partition.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) -.
↪..
OID:1.3.6.1.4.1.25623.1.0.809813
Version used: 2022-04-25T14:50:49Z

**Product Detection Result**
Product: cpe:/a:mysql:mysql:5.5.20-log
Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)
OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**
cve: CVE-2013-1502
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59239
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798

[ return to 172.16.1.8 ]