Scan Report

December 11, 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 "Scan Actual Working Shit". The scan started at Mon Dec 11 18:09:49 2023 UTC and ended at Mon Dec 11 19:06:27 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.15	8	13	3	0	0
10.0.2.4	38	115	14	0	0
10.0.2.2	0	1	0	0	0
Total: 3	46	129	17	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 192 results selected by the filtering described above. Before filtering there were 744 results.

1.1 Host Authentications

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

2 Results per Host

2.1 10.0.2.15

Host scan start	Mon Dec 11 18:10:04 2023 UTC
Host scan end	Mon Dec 11 18:57:56 2023 UTC

Service (Port)	Threat Level
80/tcp	High
22/tcp	High
21/tcp	High
631/tcp	High
80/tcp	Medium
22/tcp	Medium
21/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
631/tcp	Medium
22/tcp	Low
general/icmp	Low
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check

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

Quality of Detection: 95

Vulnerability Detection Result
`Vulnerable URL: http://10.0.2.15/drupal/sites/all/modules/coder/coder_upgrade/sc`
`↪ripts/coder_upgrade.run.php`

Solution:
Solution type: VendorFix
Install the latest version.

Vulnerability Insight
The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

Vulnerability Detection Method
Checks for known error message from affected modules.
Details: `Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105818
Version used: `2023-07-21T05:05:22Z`

References
`url: https://www.drupal.org/node/2765575`

High (CVSS: 7.5)
NVT: Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

Summary

... continues on next page ...

... continued from previous page ...

Drupal is prone to an SQL injection (SQLi) vulnerability.

Quality of Detection: 98

Vulnerability Detection Result
`Vulnerable URL: http://10.0.2.15/drupal/?q=node&destination=node`

Impact
Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

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

Affected Software/OS
Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight
Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method
Sends a special crafted HTTP POST request and checks the response.
Details: `Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105101
Version used: `2023-07-26T05:05:09Z`

References
`cve: CVE-2014-3704`
`url: https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-cor`
`↪e/2014-10-15/sa-core-2014-005-drupal-core-sql`
`url: http://www.securityfocus.com/bid/70595`
`cert-bund: CB-K14/1301`
`cert-bund: CB-K14/0920`
`dfn-cert: DFN-CERT-2014-1369`
`dfn-cert: DFN-CERT-2014-0958`

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 99

Vulnerability Detection Result
We could upload the following files via the PUT method at this web server:
http://10.0.2.15/uploads/puttest439891714.html
We could delete the following files via the DELETE method at this web server:
http://10.0.2.15/uploads/puttest439891714.html

Impact
- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution:
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Affected Software/OS
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method
Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Details: Test HTTP dangerous methods
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: 2023-08-01T13:29:10Z

References
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001

[return to 10.0.2.15]

2.1.2 High 22/tcp

High (CVSS: 7.8)
NVT: SSH Brute Force Logins With Default Credentials Reporting

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

Quality of Detection: 95

... continues on next page ...

... continued from previous page ...

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

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

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

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

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: SSH Brute Force Logins With Default Credentials Reporting
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: 2023-11-03T05:05:46Z

References
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2020-9473
cve: CVE-2023-1944

[return to 10.0.2.15]

2.1.3 High 21/tcp

High (CVSS: 10.0)
NVT: ProFTPD 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Product detection result
cpe:/a:proftpd:proftpd:1.3.5
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)

... continues on next page ...

... continued from previous page ...

Summary
ProFTPD is prone to an unauthenticated copying of files vulnerability.

Quality of Detection: 99

Vulnerability Detection Result
`The target was found to be vulnerable`

Impact
Under some circumstances this could result in remote code execution

Solution:
Solution type: VendorFix
Ask the vendor for an update

Vulnerability Detection Method
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO
Details: `ProFTPD 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPTO`
OID:1.3.6.1.4.1.25623.1.0.105254
Version used: `2022-12-02T10:11:16Z`

Product Detection Result
Product: `cpe:/a:proftpd:proftpd:1.3.5`
Method: `ProFTPD Server Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.900815)

References
`cve: CVE-2015-3306`
`url: http://bugs.proftpd.org/show_bug.cgi?id=4169`
`cert-bund: CB-K15/0791`
`cert-bund: CB-K15/0553`
`dfn-cert: DFN-CERT-2015-0839`
`dfn-cert: DFN-CERT-2015-0576`

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

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

Quality of Detection: 95

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

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
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: FTP Brute Force Logins Reporting
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: 2023-12-06T05:06:11Z

References
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2017-8218
cve: CVE-2018-19063
cve: CVE-2018-19064

[return to 10.0.2.15]

2.1.4 High 631/tcp

High (CVSS: 7.8)
NVT: CUPS < 2.4.3 DoS Vulnerability

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

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 1.7.2
Fixed version:     2.4.3
```

Solution:
Solution type: VendorFix
Update to version 2.4.3 or later.

Affected Software/OS
CUPS prior to version 2.4.3.

Vulnerability Insight
A buffer overflow vulnerability in the function format_log_line could allow remote attackers to cause a denial-of-service(DoS) on the affected system. Exploitation of the vulnerability can be triggered when the configuration file cupsd.conf sets the value of loglevel to DEBUG.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `CUPS < 2.4.3 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.170542
Version used: `2023-08-16T05:05:28Z`

References
```
cve: CVE-2023-32324
url: https://github.com/OpenPrinting/cups/security/advisories/GHSA-cxc6-w2g7-69p
↪7
url: https://github.com/OpenPrinting/cups/releases/tag/v2.4.3
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1349
dfn-cert: DFN-CERT-2023-2770
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1258
```

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

Summary

. . . continues on next page . . .

... continued from previous page ...

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

Quality of Detection: 98

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
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: 2023-07-20T05:05:17Z

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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[return to 10.0.2.15]

2.1.5 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://10.0.2.15/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.15/phpmyadmin/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 1.6.2
Fixed version: 1.9.0
Installation
path / port: /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://10.0.2.15/phpmyadmin/setup/../js/jquery/jquery-1.6.2.j
↪s
- Referenced at: http://10.0.2.15/phpmyadmin/setup/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 5.0)
NVT: Drupal 7.0 Information Disclosure Vulnerability - Active Check

Summary
Drupal is prone to an information disclosure vulnerability.

Quality of Detection: 95

Vulnerability Detection Result
Vulnerable URL: http://10.0.2.15/drupal/modules/simpletest/tests/upgrade/drupal-
↪6.upload.database.php

Impact
Successful exploitation will allow attacker to obtain sensitive information that could aid in further 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
Drupal version 7.0 is known to be affected.

Vulnerability Insight
The flaw is due to insufficient error checking, allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message.

Vulnerability Detection Method
Details: Drupal 7.0 Information Disclosure Vulnerability - Active Check
OID:1.3.6.1.4.1.25623.1.0.902574
Version used: 2021-12-01T11:10:56Z

References
cve: CVE-2011-3730
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/!_README
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/drupal-7.0

Medium (CVSS: 5.0)
NVT: Unprotected Web App / Device Installers (HTTP)

Summary
The script attempts to identify installation/setup pages of various web apps/devices that are publicly accessible and not protected by e.g. account restrictions or having their setup finished.

Quality of Detection: 80

Vulnerability Detection Result
```
The following web app/device installers are unprotected/have not finished their
↪setup and are publicly accessible (URL:Description):
http://10.0.2.15/phpmyadmin/setup/index.php - CubeCart / phpMyAdmin installer
```

Impact
It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

Solution:
Solution type: Mitigation
Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it, remove it completely or finish the setup of the application / device.

Vulnerability Detection Method
Enumerate the remote web server and check if unprotected web apps/devices are accessible for installation.
Details: `Unprotected Web App / Device Installers (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107307
Version used: `2023-07-20T05:05:17Z`

Medium (CVSS: 5.0)
NVT: Sensitive File Disclosure (HTTP)

Summary
The script attempts to identify files containing sensitive data at the remote web server.

Quality of Detection: 70

Vulnerability Detection Result
```
The following files containing sensitive information were identified:
Description:   Microsoft IIS / ASP.NET Core Module web.config file accessible. T
↪his could contain sensitive information about the structure of the application
↪ / web server and shouldn't be accessible.
Match:         <configuration>
  <system.webServer>
Used regex:    ^\s*<(configuration|system\.web(Server)?)>
```

... continues on next page ...

... continued from previous page ...

```
Extra match 1:   </system.webServer>
</configuration>
Used regex:    ^\s*</(configuration|system\.web(Server)?)>
URL:           http://10.0.2.15/drupal/web.config
```

Impact
Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

Solution:
Solution type: Mitigation
The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Insight
Currently the script is checking for files like e.g.:
- software (Blog, CMS) configuration or log files
- web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...)
- Cloud (e.g. AWS) configuration files
- database backup files
- SSH or SSL/TLS Private Keys

Vulnerability Detection Method
Enumerate the remote web server and check if sensitive files are accessible.
Details: `Sensitive File Disclosure (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107305
Version used: `2023-08-04T05:06:23Z`

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

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

Quality of Detection: 80

Vulnerability Detection Result

```
The following input fields were identified (URL:input name):
http://10.0.2.15/drupal/:pass
http://10.0.2.15/drupal/?D=A:pass
http://10.0.2.15/payroll_app.php:password
http://10.0.2.15/phpmyadmin/:pma_password
http://10.0.2.15/phpmyadmin/?D=A:pma_password
```

... continues on next page ...

... continued from previous page ...

http://10.0.2.15/phpmyadmin/changelog.php:pma_password
http://10.0.2.15/phpmyadmin/index.php:pma_password
http://10.0.2.15/phpmyadmin/license.php:pma_password
http://10.0.2.15/phpmyadmin/url.php:pma_password

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

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

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

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-07-20T05:05:17Z

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: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://10.0.2.15/phpmyadmin/setup/../js/jquery/jquery-1.6.2.j
↪s
- Referenced at:   http://10.0.2.15/phpmyadmin/setup/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
```

... continues on next page ...

... continued from previous page ...

```
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://10.0.2.15/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.15/phpmyadmin/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2011-4969`
`url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/`
`cert-bund: CB-K17/0195`
`dfn-cert: DFN-CERT-2017-0199`
`dfn-cert: DFN-CERT-2016-0890`

[return to 10.0.2.15]

2.1.6 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSH server supports the following weak host key algorithm(s):`
`host key algorithm | Description`

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪---------
ssh-dss             | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)

... continues on next page ...

... continued from previous page ...

- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2023-10-12T05:05:32Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
```

... continues on next page ...

... continued from previous page ...

```
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[return to 10.0.2.15]

2.1.7 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Anonymous login ok, send your complete email address
↪ as your password
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-10-13T05:06:09Z`

[return to 10.0.2.15]

2.1.8 Medium 631/tcp

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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

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

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

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more 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: 2023-10-20T16:09:12Z

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↪-report-2014

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 10.0.2.15]

2.1.9 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 10.0.2.15]

2.1.10 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.2.15]

2.1.11 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 432158
Packet 2: 432420
```

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.

... continues on next page ...

... continued from previous page ...

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-08-01T13:29:10Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[return to 10.0.2.15]

2.2 10.0.2.4

Host scan start Mon Dec 11 18:10:04 2023 UTC
Host scan end Mon Dec 11 19:06:22 2023 UTC

Service (Port)	Threat Level
21/tcp	High
9200/tcp	High
3306/tcp	High
1617/tcp	High
4848/tcp	High
22/tcp	High
8383/tcp	High
21/tcp	Medium
9200/tcp	Medium
3306/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
8181/tcp	Medium
135/tcp	Medium
4848/tcp	Medium
22/tcp	Medium
3389/tcp	Medium
8383/tcp	Medium
general/icmp	Low
9200/tcp	Low
3306/tcp	Low
general/tcp	Low
22/tcp	Low

2.2.1 High 21/tcp

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

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

Quality of Detection: 95

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

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

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

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices
Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-12-06T05:06:11Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2001-1594`
`cve: CVE-2013-7404`
`cve: CVE-2017-8218`
`cve: CVE-2018-19063`
`cve: CVE-2018-19064`

[return to 10.0.2.4]

2.2.2 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.

Quality of Detection: 80

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

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

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-20T05:05:17Z`

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.

Quality of Detection: 80

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

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

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.6.1, or later.

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808091
Version used: `2023-07-20T05:05:17Z`

References

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 5.6.12

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

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

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

Vulnerability Insight
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: 2023-07-20T05:05:17Z

References
cve: CVE-2018-3831
url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update
↪/149035

... continues on next page ...

... continued from previous page ...

url: https://www.elastic.co/community/security
dfn-cert: DFN-CERT-2020-1653

[return to 10.0.2.4]

2.2.3 High 3306/tcp

High (CVSS: 10.0)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows

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

Summary
Oracle MySQL Server is prone to a vulnerability in libcurl.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.41
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior and 8.0 through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149170
Version used: 2023-01-20T10:11:50Z

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-2022-32221
cve: CVE-2022-35260
cve: CVE-2022-42915
cve: CVE-2022-42916
url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL
advisory-id: cpujan2023
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1026
cert-bund: WID-SEC-2023-0296
cert-bund: WID-SEC-2023-0189
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1862
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1636
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0278
dfn-cert: DFN-CERT-2023-0216
dfn-cert: DFN-CERT-2023-0214
dfn-cert: DFN-CERT-2023-0157
dfn-cert: DFN-CERT-2023-0156
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2401
dfn-cert: DFN-CERT-2022-2400
dfn-cert: DFN-CERT-2022-2393
dfn-cert: DFN-CERT-2022-2391

High (CVSS: 10.0)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

Product detection result

... 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 vulnerability in InnoDB (zlib).

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.42
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149536
Version used: 2023-04-19T10:19:33Z

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

References
cve: CVE-2022-37434
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1728

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1031
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0140
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2023-0125
cert-bund: WID-SEC-2022-1888
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0929
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2421
dfn-cert: DFN-CERT-2022-2415
dfn-cert: DFN-CERT-2022-2366
dfn-cert: DFN-CERT-2022-2365
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2363
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-1841
dfn-cert: DFN-CERT-2022-1710
```

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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

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-2023-2723
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0141

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0736
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0277
cert-bund: WID-SEC-2022-0071
cert-bund: WID-SEC-2022-0005
cert-bund: CB-K22/0619
cert-bund: CB-K22/0570
cert-bund: CB-K22/0536
cert-bund: CB-K22/0386
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2150

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2066
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1992
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1875
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1614
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1310
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1049
dfn-cert: DFN-CERT-2022-0986
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716
```

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

Product detection result

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

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

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
Product: cpe:/a:mysql:mysql:5.5.20-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-2023-2229
cert-bund: WID-SEC-2023-1821
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1030

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-0530
cert-bund: WID-SEC-2022-2354
cert-bund: WID-SEC-2022-2000
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1515
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0874
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0473
cert-bund: CB-K22/0469
cert-bund: CB-K22/0316
cert-bund: CB-K22/0224
cert-bund: CB-K22/0077
cert-bund: CB-K22/0072
cert-bund: CB-K22/0062
cert-bund: CB-K22/0045
cert-bund: CB-K22/0030
cert-bund: CB-K22/0011
cert-bund: CB-K21/1268
cert-bund: CB-K21/1179
cert-bund: CB-K21/1161
cert-bund: CB-K21/1087
cert-bund: CB-K21/0994
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
cert-bund: CB-K21/0907
cert-bund: CB-K21/0897
cert-bund: CB-K21/0797
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-2825
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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

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

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

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

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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

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

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

References
`cve: CVE-2018-3133`
`cve: CVE-2018-3174`
`cve: CVE-2018-3282`
`cve: CVE-2016-9843`
`cve: CVE-2016-9840`
`cve: CVE-2016-9841`
`cve: CVE-2016-9842`
`url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixMSQL`
`advisory-id: cpuoct2018`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0714`
`cert-bund: CB-K18/1005`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K18/0030`
`cert-bund: CB-K17/2199`
`cert-bund: CB-K17/2168`
`cert-bund: CB-K17/1745`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1622`
`cert-bund: CB-K17/1585`
`cert-bund: CB-K17/1062`
`cert-bund: CB-K17/0877`
`cert-bund: CB-K17/0784`
`cert-bund: CB-K16/1996`
`dfn-cert: DFN-CERT-2020-1536`
`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-2019-0592
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.

Quality of Detection: 80

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`
`cert-bund: CB-K16/1392`

... continues on next page ...

... continued from previous page ...

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: 9.0)
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.

Quality of Detection: 80

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

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

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

Affected Software/OS
Oracle MySQL version 5.1.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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803111
Version used: 2023-07-25T05:05:58Z

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

High (CVSS: 8.1)
NVT: Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.35

... continues on next page ...

... continued from previous page ...

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

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

References
`cve: CVE-2021-22901`
`cve: CVE-2019-17543`
`cve: CVE-2021-2389`
`cve: CVE-2021-2390`
`cve: CVE-2021-2356`
`cve: CVE-2021-2385`
`cve: CVE-2021-2342`
`cve: CVE-2021-2372`
`cve: CVE-2021-22897`
`cve: CVE-2021-22898`
`url: https://www.oracle.com/security-alerts/cpujul2021.html#AppendixMSQL`
`advisory-id: cpujul2021`
`cert-bund: WID-SEC-2023-2229`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-0063`
`cert-bund: WID-SEC-2022-1963`
`cert-bund: WID-SEC-2022-0873`
`cert-bund: CB-K22/0044`
`cert-bund: CB-K21/0813`
`cert-bund: CB-K21/0770`
`dfn-cert: DFN-CERT-2022-1892`
`dfn-cert: DFN-CERT-2022-1692`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2369
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-1743
dfn-cert: DFN-CERT-2021-1677
dfn-cert: DFN-CERT-2021-1593
dfn-cert: DFN-CERT-2021-1580
dfn-cert: DFN-CERT-2021-1537
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-1174
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-1157
dfn-cert: DFN-CERT-2021-1151
dfn-cert: DFN-CERT-2021-1148
dfn-cert: DFN-CERT-2021-1045
dfn-cert: DFN-CERT-2019-2216
```

High (CVSS: 8.1)
NVT: Oracle MySQL Server <= 5.5.49 / 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.

Quality of Detection: 80

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 confidentiality, integrity, and availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server versions 5.5.49 and prior, 5.6 through 5.6.30 and 5.7 through 5.7.12.

Vulnerability Insight
Multiple unspecified errors exist in the 'MySQL Server' component via unknown vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.808588
Version used: `2023-11-03T05:05:46Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-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`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1849
dfn-cert: DFN-CERT-2016-1540
dfn-cert: DFN-CERT-2016-1217
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-1169

High (CVSS: 7.8)
NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

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

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

Quality of Detection: 95

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

Solution:
Solution type: Mitigation
- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

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

Other products might be affected as well.

Vulnerability Detection Method
Details: MySQL / MariaDB Default Credentials (MySQL Protocol)
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: 2023-04-17T10:19:34Z

... 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-2001-0645
cve: CVE-2004-2357
cve: CVE-2006-1451
cve: CVE-2007-2554
cve: CVE-2007-6081
cve: CVE-2009-0919
cve: CVE-2014-3419
cve: CVE-2015-4669
cve: CVE-2016-6531
cve: CVE-2018-15719

High (CVSS: 7.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.42
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.33 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.

... 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 <= 5.7.41, 8.x <= 8.0.32 Security Update (cpuapr2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149538
Version used: 2023-04-19T10:19:33Z

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

References
cve: CVE-2023-0215
cve: CVE-2022-43551
cve: CVE-2023-21980
cve: CVE-2022-4304
cve: CVE-2022-4450
cve: CVE-2023-0286
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1886
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1793
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1553
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0777
cert-bund: WID-SEC-2023-0304
cert-bund: WID-SEC-2022-2375
dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1462

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-1043
dfn-cert: DFN-CERT-2023-1037
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0774
dfn-cert: DFN-CERT-2023-0685
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2023-0618
dfn-cert: DFN-CERT-2023-0543
dfn-cert: DFN-CERT-2023-0471
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0318
dfn-cert: DFN-CERT-2023-0310
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0288
dfn-cert: DFN-CERT-2023-0284
dfn-cert: DFN-CERT-2023-0283
dfn-cert: DFN-CERT-2022-2902
```

High (CVSS: 7.8)
NVT: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Windows

Product detection result

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

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.42
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.31 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.30.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.30 Security Update (cpuapr2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149534
Version used: 2023-04-19T10:19:33Z

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

References
cve: CVE-2023-21912
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1033
dfn-cert: DFN-CERT-2023-1058
dfn-cert: DFN-CERT-2023-1037
dfn-cert: DFN-CERT-2023-0885

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

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

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

Quality of Detection: 80

... 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 attackers to cause the affected application to crash, resulting in a denial-of-service condition.

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

Affected Software/OS
Oracle MySQL version 5.5.54 and earlier, 5.6.20 and earlier on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows
OID:1.3.6.1.4.1.25623.1.0.810880
Version used: 2023-07-14T16:09:27Z

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

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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.5.39 / 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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.40
Installation
path / port: 3306/tcp

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

Solution:
Solution type: VendorFix
Update to version 5.5.40, 5.6.21 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5.39 and prior and 5.6 through 5.6.20.

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

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

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2014-1357

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

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

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

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

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

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

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

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: 2023-07-25T05:05:58Z

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-2015-0411
cve: CVE-2014-6568

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2015-0382
cve: CVE-2015-0381
cve: CVE-2015-0374
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72191
url: http://www.securityfocus.com/bid/72210
url: http://www.securityfocus.com/bid/72200
url: http://www.securityfocus.com/bid/72214
url: http://www.securityfocus.com/bid/72227
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074
```

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

Product detection result

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

Summary

Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.38
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.38, 8.0.29 or later.

... continues on next page ...

... continued from previous page ...

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-2023-1969`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-1081`
`cert-bund: WID-SEC-2022-1057`
`cert-bund: WID-SEC-2022-0836`
`cert-bund: WID-SEC-2022-0833`
`cert-bund: WID-SEC-2022-0826`
`cert-bund: WID-SEC-2022-0767`
`cert-bund: WID-SEC-2022-0677`
`cert-bund: WID-SEC-2022-0551`
`cert-bund: WID-SEC-2022-0530`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0393`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: WID-SEC-2022-0270`
`cert-bund: WID-SEC-2022-0261`
`cert-bund: WID-SEC-2022-0200`
`cert-bund: WID-SEC-2022-0190`
`cert-bund: WID-SEC-2022-0169`

... continues on next page ...

... continued from previous page ...

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-2023-2667
dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2094
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-2047
dfn-cert: DFN-CERT-2022-1928
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1667
dfn-cert: DFN-CERT-2022-1597
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1370
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1205
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603

High (CVSS: 7.5)
NVT: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - 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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.34
Installation
path / port: 3306/tcp

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.145796
Version used: 2023-10-20T16:09:12Z

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-2021-2307
cve: CVE-2021-3449
cve: CVE-2021-3450
cve: CVE-2021-23840
cve: CVE-2021-23841
cve: CVE-2021-2304
cve: CVE-2021-2180
cve: CVE-2021-2194
cve: CVE-2021-2166
cve: CVE-2021-2179

... continues on next page ...

... continued from previous page ...

```
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-2023-0065
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1320
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1294
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0671
cert-bund: WID-SEC-2022-0669
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K22/0476
cert-bund: CB-K22/0061
cert-bund: CB-K21/1097
cert-bund: CB-K21/1095
cert-bund: CB-K21/1065
cert-bund: CB-K21/0785
cert-bund: CB-K21/0770
cert-bund: CB-K21/0573
cert-bund: CB-K21/0572
cert-bund: CB-K21/0565
cert-bund: CB-K21/0421
cert-bund: CB-K21/0412
cert-bund: CB-K21/0409
cert-bund: CB-K21/0389
cert-bund: CB-K21/0317
cert-bund: CB-K21/0185
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0933
dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2216
```

... continues on next page ...

... continued from previous page ...

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

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

... continues on next page ...

... continued from previous page ...

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

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

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

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

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

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

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

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

References

... continues on next page ...

... continued from previous page ...

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

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

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

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

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

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

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

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-2020-1967
cve: CVE-2020-14539
cve: CVE-2020-14559
url: https://www.oracle.com/security-alerts/cpujul2020.html#AppendixMSQL
advisory-id: cpujul2020
cert-bund: WID-SEC-2023-3080
cert-bund: CB-K21/1088
cert-bund: CB-K21/0070
cert-bund: CB-K20/1023
cert-bund: CB-K20/1017
cert-bund: CB-K20/0711
cert-bund: CB-K20/0708
cert-bund: CB-K20/0357
dfn-cert: DFN-CERT-2021-2192
dfn-cert: DFN-CERT-2021-0830
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0140
dfn-cert: DFN-CERT-2020-2295
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1788
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-0956
dfn-cert: DFN-CERT-2020-0930
dfn-cert: DFN-CERT-2020-0841
dfn-cert: DFN-CERT-2020-0824
dfn-cert: DFN-CERT-2020-0822
```

High (CVSS: 7.5)
NVT: Oracle MySQL 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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.21
Installation
path / port: 3306/tcp

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

Solution:
Solution type: VendorFix
Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.

Affected Software/OS
Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Windows

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.810603
Version used: 2023-07-25T05:05:58Z

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-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

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1239
cert-bund: CB-K17/0657
cert-bund: CB-K17/0423
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0430
```

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

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

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

Quality of Detection: 80

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

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

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

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

... 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-2021-2144
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2021-0821

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

Quality of Detection: 80

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

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

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

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-20T05:05:17Z`

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

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

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.

Quality of Detection: 80

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

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

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-25T05:05:58Z`

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

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

... continues on next page ...

... continued from previous page ...

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

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

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

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

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

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

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

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

References
cve: CVE-2016-0609

... continues on next page ...

... continued from previous page ...

```
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

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

Summary

... continues on next page ...

... continued from previous page ...

Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

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

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

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (...
OID:1.3.6.1.4.1.25623.1.0.112489
Version used: 2023-02-02T10:09:00Z

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

References
cve: CVE-2019-2534
cve: CVE-2019-2529
cve: CVE-2019-2482
cve: CVE-2019-2455
cve: CVE-2019-2503

... continues on next page ...

... continued from previous page ...

cve: CVE-2018-0734
cve: CVE-2019-2537
cve: CVE-2019-2481
cve: CVE-2019-2507
cve: CVE-2019-2531
cve: CVE-2018-5407
url: https://www.oracle.com/security-alerts/cpujan2019.html#AppendixMSQL
advisory-id: cpujan2019
cert-bund: WID-SEC-2023-3083
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-1696
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K22/0045
cert-bund: CB-K20/0324
cert-bund: CB-K20/0136
cert-bund: CB-K19/1121
cert-bund: CB-K19/0696
cert-bund: CB-K19/0622
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0318
cert-bund: CB-K19/0316
cert-bund: CB-K19/0314
cert-bund: CB-K19/0050
cert-bund: CB-K19/0044
cert-bund: CB-K18/1173
cert-bund: CB-K18/1065
cert-bund: CB-K18/1039
dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2305
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1600
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1455

... continues on next page ...

... continued from previous page ...

```
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.

Quality of Detection: 80

Vulnerability Detection Result

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

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation of this vulnerability will allow remote attackers to 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: `2023-07-20T05:05:18Z`

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation of 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)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

cve: CVE-2016-6663
cve: CVE-2016-6664
cve: CVE-2016-3492
cve: CVE-2016-5626
cve: CVE-2016-5629
cve: CVE-2016-5616
cve: CVE-2016-5617
cve: CVE-2016-8283
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0139
cert-bund: CB-K16/1979
cert-bund: CB-K16/1846
cert-bund: CB-K16/1755
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0138
dfn-cert: DFN-CERT-2016-2089
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1859
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714

[return to 10.0.2.4]

2.2.4 High 1617/tcp

High (CVSS: 7.5)
NVT: Java JMX Insecure Configuration Vulnerability

Summary

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

Quality of Detection: 70

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the ↪ RMI port 49163/tcp without providing any credentials.

Solution:
Solution type: Mitigation
Enable password authentication and/or SSL client certificate authentication for the JMX agent.

Vulnerability Detection Method
Sends crafted RMI requests and checks the responses.
Details: Java JMX Insecure Configuration Vulnerability
OID:1.3.6.1.4.1.25623.1.0.143207
Version used: 2020-11-10T09:46:51Z

References
url: https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/
url: https://www.optiv.com/blog/exploiting-jmx-rmi
url: https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server

[return to 10.0.2.4]

2.2.5 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.

Quality of Detection: 99

Vulnerability Detection Result
Vulnerable URL: https://10.0.2.4:4848/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.

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Send a crafted request via HTTP GET and check whether it is able to get the content of passwd file.
Details: `Oracle Glass Fish Server Directory Traversal Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806848
Version used: `2023-07-20T05:05:17Z`

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

[return to 10.0.2.4]

2.2.6 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.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: 7.2`
`Installation`
`path / port: 22/tcp`

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

... 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: `2023-07-14T16:09:27Z`

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

References
`cve: CVE-2016-1908`
`url: http://openwall.com/lists/oss-security/2016/01/15/13`
`url: http://www.securityfocus.com/bid/84427`
`url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4`
`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: 7.8)
NVT: SSH Brute Force Logins With Default Credentials Reporting

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

Quality of Detection: 95

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

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

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

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

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2023-11-03T05:05:46Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2020-9473`
`cve: CVE-2023-1944`

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

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

... continues on next page ...

... continued from previous page ...

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

Quality of Detection: 80

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

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

Solution:
Solution type: VendorFix
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: `2023-07-20T05:05:17Z`

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

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-6515
cve: CVE-2016-6210
url: http://www.openssh.com/txt/release-7.3
url: http://www.securityfocus.com/bid/92212
url: http://seclists.org/fulldisclosure/2016/Jul/51
url: https://security-tracker.debian.org/tracker/CVE-2016-6210
url: http://openwall.com/lists/oss-security/2016/08/01/2
cert-bund: WID-SEC-2023-0450
cert-bund: WID-SEC-2023-0449
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1753
cert-bund: CB-K17/1349
cert-bund: CB-K17/1292
cert-bund: CB-K17/0055
cert-bund: CB-K16/1837
cert-bund: CB-K16/1629
cert-bund: CB-K16/1487
cert-bund: CB-K16/1485
cert-bund: CB-K16/1252
cert-bund: CB-K16/1221
cert-bund: CB-K16/1082
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1407
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1729
dfn-cert: DFN-CERT-2016-1576
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-1331
dfn-cert: DFN-CERT-2016-1243
dfn-cert: DFN-CERT-2016-1149
```

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

Product detection result

... continues on next page ...

... continued from previous page ...

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

Summary
openssh is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 7.1
Fixed version: 7.4
Installation
path / port: 22/tcp

Impact
Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a 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: 2023-07-25T05:05:58Z

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

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

cve: CVE-2016-10009
cve: CVE-2016-10010
cve: CVE-2016-10011
cve: CVE-2016-10012
cve: CVE-2016-10708
url: https://www.openssh.com/txt/release-7.4
url: http://www.securityfocus.com/bid/94968
url: http://www.securityfocus.com/bid/94972
url: http://www.securityfocus.com/bid/94977
url: http://www.securityfocus.com/bid/94975
url: http://www.openwall.com/lists/oss-security/2016/12/19/2
url: http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
url: https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93
↪3e6b931de1d16737
cert-bund: WID-SEC-2023-1996
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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-1096
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0386
dfn-cert: DFN-CERT-2017-0130
dfn-cert: DFN-CERT-2017-0042
dfn-cert: DFN-CERT-2016-2099
```

[return to 10.0.2.4]

2.2.7 High 8383/tcp

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.

Quality of Detection: 98

Vulnerability Detection Result

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

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

... continues on next page ...

... continued from previous page ...

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: 2023-07-20T05:05:17Z

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

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
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
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[return to 10.0.2.4]

2.2.8 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection: 70

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Password required for anonymous.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-10-13T05:06:09Z`

[return to 10.0.2.4]

2.2.9 Medium 9200/tcp

Medium (CVSS: 6.8)
NVT: Elastisearch Remote Code Execution Vulnerability

Summary
Elasticsearch is prone to a remote-code-execution vulnerability.

Quality of Detection: 99

Vulnerability Detection Result
```
Vulnerable URL: http://10.0.2.4:9200/_search?source=%7B%22size%22%3A1%2C%22query
↪%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%7D%7
↪D%2C%22script_fields%22%3A%7B%22VTTest%22%3A%7B%22script%22%3A%22import%20java
↪.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2Fwindo
↪ws%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D%7
↪D%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

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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 < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability (Windows)

Summary
Elasticsearch is prone to a field disclosure vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.12
Installation
path / port:       /
```

Impact
An attacker could gain additional permissions against a restricted index.

Solution:
Solution type: VendorFix
Update to version 6.8.12, 7.9.1 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.12 and 7.9.0.

Vulnerability Insight
A field disclosure flaw was found in Elasticsearch when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 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: 6.5)
NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

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

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.17
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 6.8.17, 7.13.3 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.17 and 7.x prior to 7.13.3.

Vulnerability Insight
An uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)`
OID:1.3.6.1.4.1.25623.1.0.146386
Version used: `2021-08-17T12:00:57Z`

... continues on next page ...

... continued from previous page ...

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: 5.9)
NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) (Windows)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 6.8.2
Installation
path / port: /

Impact
On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

Solution:
Solution type: VendorFix
Update to version 6.8.2 or 7.2.1 respectively.

Affected Software/OS
Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.

Vulnerability Insight
A race condition flaw was found in the response headers Elasticsearch returns to a request.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability.
↪..
OID:1.3.6.1.4.1.25623.1.0.117162
Version used: 2023-03-06T10:19:58Z

References
cve: CVE-2019-7614

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 6.8.15
Installation
path / port: /

Impact
This could lead to disclosing the existence of documents and fields the attacker should not be able to view or result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.15, 7.12.0 or later.

Affected Software/OS
Elasticsearch versions prior to versions 6.8.15 or 7.12.0.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-22135: Suggester & Profile API information disclosure flaw
- CVE-2021-22137: Field disclosure flaw

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)
OID:1.3.6.1.4.1.25623.1.0.145940
Version used: 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-update/268125

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 6.8.14
Installation
path / port: /

Impact
This could allow an Elasticsearch administrator to view sensitive details.

Solution:
Solution type: VendorFix
Update to version 6.8.14, 7.10.0 or later.

Affected Software/OS
Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.

Vulnerability Insight
Elasticsearch has an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)
OID:1.3.6.1.4.1.25623.1.0.145383
Version used: 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.

Quality of Detection: 80

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: `2023-07-21T05:05:22Z`

References
`cve: CVE-2014-6439`
`url: https://www.elastic.co/community/security/`
`url: http://www.securityfocus.com/bid/70233`
`url: http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded`

[return to 10.0.2.4]

2.2.10 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: MySQL Server Components Multiple Unspecified Vulnerabilities

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
MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20-log
Fixed version: See advisory

Impact
Successful exploitation could allow remote authenticated users to affect availability via unknown vectors.

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

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: 2023-07-27T05:05:08Z

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-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

... continues on next page ...

... continued from previous page ...

```
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 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.

Quality of Detection: 80

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

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

Solution:
Solution type: VendorFix
Apply the patch from the references or upgrade to latest version.

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.65 and Oracle MySQL version 5.5.x to 5.5.27 on Windows.

Vulnerability Insight
The flaws are due to multiple unspecified errors in MySQL server component related to server installation and server optimizer.

Vulnerability Detection Method
Details: `Oracle MySQL Server Multiple Vulnerabilities-02 Nov12 (Windows)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.803112
Version used: 2023-07-25T05:05:58Z

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-2012-3180
cve: CVE-2012-3177
cve: CVE-2012-3160
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56003
url: http://www.securityfocus.com/bid/56005
url: http://www.securityfocus.com/bid/56027
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1
dfn-cert: DFN-CERT-2012-2200
dfn-cert: DFN-CERT-2012-2118

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.67, 5.5.29 or later.

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.5.29 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.28.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.28 Security Update (cpujan2013) - Windows
OID:1.3.6.1.4.1.25623.1.0.117205
Version used: 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

... continues on next page ...

... continued from previous page ...

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 5.5.x <= 5.5.23 Security Update (cpujul2012) - Windows

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

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.24
Installation
path / port: 3306/tcp

Impact
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'InnoDB' package / privilege.

Solution:
Solution type: VendorFix
Update to version 5.5.24 or later.

Affected Software/OS
Oracle MySQL Server 5.5.x through 5.5.23.

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

... continues on next page ...

... continued from previous page ...

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

References
cve: CVE-2012-1735
cve: CVE-2012-1757
cve: CVE-2012-1756
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2012-1389

Medium (CVSS: 6.8)
NVT: Oracle MySQL Server <= 5.1.65 / 5.5 <= 5.5.27 Security Update (cpujan2013) - Windows

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.28
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.66, 5.5.28 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.65 and prior and 5.5 through 5.5.27.

Vulnerability Insight
The flaw allows remote authenticated users to affect availability, related to GIS Extension.

... 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 <= 5.1.65 / 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: 6.6)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows

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

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation of this vulnerability will allow remote attackers to have impact on availability, confidentiality and integrity.

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-25T05:05:58Z`

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-2017-3309`
`cve: CVE-2017-3308`
`cve: CVE-2017-3329`
`cve: CVE-2017-3456`
`cve: CVE-2017-3453`
`cve: CVE-2017-3600`
`cve: CVE-2017-3462`
`cve: CVE-2017-3463`
`cve: CVE-2017-3461`
`cve: CVE-2017-3464`
`url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html`
`url: http://www.securityfocus.com/bid/97742`
`url: http://www.securityfocus.com/bid/97725`
`url: http://www.securityfocus.com/bid/97763`
`url: http://www.securityfocus.com/bid/97831`
`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`

... continues on next page ...

... continued from previous page ...

```
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 Server <= 5.1.67 / 5.5 <= 5.5.29 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

Product detection result

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

Summary

Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Update to version 5.1.68, 5.5.30, 5.6.11 or later.

... continues on next page ...

... continued from previous page ...

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
`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 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.

Quality of Detection: 80

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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-2014-4258`
`cve: CVE-2014-4260`
`url: http://secunia.com/advisories/59521`
`url: http://www.securityfocus.com/bid/68564`
`url: http://www.securityfocus.com/bid/68573`
`url: http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_securi`
`↪ty_patches`
`url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#A`
`↪ppendixMSQL`
`cert-bund: CB-K15/0567`
`cert-bund: CB-K14/1420`
`cert-bund: CB-K14/0891`
`cert-bund: CB-K14/0868`
`dfn-cert: DFN-CERT-2015-0593`
`dfn-cert: DFN-CERT-2014-1500`
`dfn-cert: DFN-CERT-2014-0930`
`dfn-cert: DFN-CERT-2014-0911`

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)

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

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.5.36 and earlier and 5.6.16 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Performance Schema, Options, RBR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804575
Version used: 2023-07-26T05:05:09Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-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

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2014-2436
cve: CVE-2014-2440
url: http://secunia.com/advisories/57940
url: http://www.securityfocus.com/bid/66850
url: http://www.securityfocus.com/bid/66858
url: http://www.securityfocus.com/bid/66890
url: http://www.securityfocus.com/bid/66896
url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638
url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0464
cert-bund: CB-K14/0452
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0477
dfn-cert: DFN-CERT-2014-0459
```

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows

Product detection result

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

Summary

Oracle MySQL is prone to multiple denial-of-service vulnerabilities.

Quality of Detection: 80

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-20T05:05:18Z`

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-2018-2668`
`cve: CVE-2018-2665`
`cve: CVE-2018-2622`
`cve: CVE-2018-2640`
`url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html`
`cert-bund: CB-K18/0480`
`cert-bund: CB-K18/0392`
`cert-bund: CB-K18/0265`
`cert-bund: CB-K18/0096`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-1265`
`dfn-cert: DFN-CERT-2018-0515`
`dfn-cert: DFN-CERT-2018-0424`
`dfn-cert: DFN-CERT-2018-0286`
`dfn-cert: DFN-CERT-2018-0101`

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows

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

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation of this vulnerability will allow remote attackers to compromise availability of the system.

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

Affected Software/OS
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.11 and earlier on Windows.

Vulnerability Insight
The flaw exists due to an error in 'Server: Optimizer'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811986
Version used: `2023-07-25T05:05:58Z`

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-2017-10378`
`url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html`
`url: http://www.securityfocus.com/bid/101375`
`cert-bund: CB-K18/0480`
`cert-bund: CB-K18/0242`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/2048`
`cert-bund: CB-K17/1748`

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 6.5)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows

Product detection result

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

Summary

Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

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

Impact

Successful exploitation of this vulnerability will allow remote to compromise availability confidentiality, and integrity of the system.

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

Affected Software/OS

Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.19 and earlier on Windows.

Vulnerability Insight

Multiple flaws exist due to:
- An error in 'Client programs' component.
- An error in 'Server: DDL'.
- An error in 'Server: Replication'

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.811991
Version used: 2023-07-14T16:09:27Z

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

References
cve: CVE-2017-10379
cve: CVE-2017-10384
cve: CVE-2017-10268
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101415
url: http://www.securityfocus.com/bid/101406
url: http://www.securityfocus.com/bid/101390
cert-bund: CB-K18/0480
cert-bund: CB-K18/0242
cert-bund: CB-K18/0224
cert-bund: CB-K17/2048
cert-bund: CB-K17/1748
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0515
dfn-cert: DFN-CERT-2018-0260
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-2137
dfn-cert: DFN-CERT-2017-1827

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.66 / 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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.29
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.1.67, 5.5.29 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.66 and prior and 5.5 through 5.5.28.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.66 / 5.5 <= 5.5.28 Security Update (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 <= 5.1.68 / 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)

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     5.5.31
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.69, 5.5.31, 5.6.11 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.68 and prior, 5.5 through 5.5.30 and 5.6 through 5.6.10.

Vulnerability Insight
Unspecified error in Server Optimizer, Server Privileges, InnoDB, and in some unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.1.68 / 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117207
Version used: `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
```

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows

Product detection result

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

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.30
Installation
path / port:       3306/tcp
```

Impact
Successful exploitation could allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Update to version 5.1.68, 5.5.30 or later.

Affected Software/OS
Oracle MySQL Server versions 5.1.67 and prior and 5.5 through 5.5.29.

Vulnerability Insight
Unspecified error in Server Partition and in some unspecified vectors.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.67 / 5.5 <= 5.5.29 Security Update (cpuapr2013) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.117209
Version used: 2022-04-25T14:50:49Z

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

References
cve: CVE-2013-1521
cve: CVE-2013-1552
cve: CVE-2013-1555
cve: CVE-2012-5614
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59196
url: http://www.securityfocus.com/bid/59210
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0839
dfn-cert: DFN-CERT-2013-0798

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.5.31 / 5.6 <= 5.6.11 Security Update (cpujan2016) - Windows

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation 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`
`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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

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

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

Affected Software/OS
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`

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

References
`cve: CVE-2014-6530`

... continues on next page ...

... continued from previous page ...

```
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 Server <= 5.5.50 / 5.6 <= 5.6.31 / 5.7 <= 5.7.13 Security Update (cpuoct2016) - Windows

Product detection result

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

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

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 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.

Quality of Detection: 80

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

Impact
Successful exploitation of this vulnerability will allow a remote authenticated user to cause denial of service conditions.

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

Affected Software/OS
Oracle MySQL Server versions 5.5.51 and prior.

Vulnerability Insight
The flaw exists due to an unspecified error within the 'Server:DML' component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.51 Security Update (cpuoct2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809378
Version used: 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-2016-5624
url: https://www.oracle.com/security-alerts/cpuoct2016.html#AppendixMSQL
advisory-id: cpuoct2016
cert-bund: CB-K16/1846
cert-bund: CB-K16/1714
cert-bund: CB-K16/1624
dfn-cert: DFN-CERT-2016-1950
dfn-cert: DFN-CERT-2016-1790
dfn-cert: DFN-CERT-2016-1714
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.44 / 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.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.45
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight
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 (.`

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.142645
Version used: 2023-10-27T16:11:32Z

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-2019-2805
cve: CVE-2019-2740
cve: CVE-2019-2819
cve: CVE-2019-2739
cve: CVE-2019-2737
cve: CVE-2019-2738
url: https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
advisory-id: cpujul2019
cert-bund: CB-K19/0620
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2180
dfn-cert: DFN-CERT-2020-0658
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2019-2695
dfn-cert: DFN-CERT-2019-2656
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1568
dfn-cert: DFN-CERT-2019-1453

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (cpuoct2019) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.46
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.46, 5.7.28, 8.0.18 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.45 and prior, 5.7 through 5.7.27 and 8.0 through 8.0.17.

Vulnerability Insight
Oracle MySQL Server is prone to multiple vulnerabilities.
For further information refer to the official advisory via the referenced link.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.45 / 5.7 <= 5.7.27 / 8.0 <= 8.0.17 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.143030
Version used: 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

... continues on next page ...

... continued from previous page ...

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)

Summary
Oracle MySQL Server is prone to an unspecified denial of service vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.47
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.47 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.46 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.46 Security Update (cpujan2020) - Windows
OID:1.3.6.1.4.1.25623.1.0.143359
Version used: 2021-08-16T09:00:57Z

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-2020-2579
url: https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL
advisory-id: cpujan2020
cert-bund: CB-K20/0038
dfn-cert: DFN-CERT-2020-1827
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0096

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (cpuoct2020) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.50
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.50, 5.7.32, 8.0.22 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.49 and prior, 5.7 through 5.7.31 and 8.0 through 8.0.21.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.49 / 5.7 <= 5.7.31 / 8.0 <= 8.0.21 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.108959

... continues on next page ...

... continued from previous page ...

Version used: 2021-08-16T12:00:57Z

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

References
cve: CVE-2020-14765
cve: CVE-2020-14769
cve: CVE-2020-14812
cve: CVE-2020-14793
cve: CVE-2020-14672
cve: CVE-2020-14867
url: https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixMSQL
advisory-id: cpuoct2020
cert-bund: CB-K20/1066
cert-bund: CB-K20/1017
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2763
dfn-cert: DFN-CERT-2020-2756
dfn-cert: DFN-CERT-2020-2620
dfn-cert: DFN-CERT-2020-2380
dfn-cert: DFN-CERT-2020-2295

Medium (CVSS: 6.5)
NVT: Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.33
Installation
path / port: 3306/tcp

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.32 and prior and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpuapr2021) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.145794
Version used: `2023-10-20T16:09:12Z`

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

References
`cve: CVE-2020-1971`
`cve: CVE-2021-2178`
`cve: CVE-2021-2202`
`url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL`
`advisory-id: cpuapr2021`
`cert-bund: WID-SEC-2023-0067`
`cert-bund: WID-SEC-2023-0065`
`cert-bund: WID-SEC-2022-2047`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: WID-SEC-2022-1000`
`cert-bund: WID-SEC-2022-0585`
`cert-bund: CB-K21/1065`
`cert-bund: CB-K21/0788`
`cert-bund: CB-K21/0615`
`cert-bund: CB-K21/0421`
`cert-bund: CB-K21/0111`
`cert-bund: CB-K21/0062`
`cert-bund: CB-K21/0006`
`cert-bund: CB-K20/1217`
`dfn-cert: DFN-CERT-2022-1582`
`dfn-cert: DFN-CERT-2022-1215`
`dfn-cert: DFN-CERT-2022-0076`
`dfn-cert: DFN-CERT-2021-2190`
`dfn-cert: DFN-CERT-2021-2155`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-0924
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2021-0255
dfn-cert: DFN-CERT-2021-0134
dfn-cert: DFN-CERT-2021-0131
dfn-cert: DFN-CERT-2021-0128
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2021-0078
dfn-cert: DFN-CERT-2021-0012
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668
```

Medium (CVSS: 6.4)
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.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     Apply the patch
```

Impact

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

Solution:

... continues on next page ...

... continued from previous page ...

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: `2023-07-25T05:05:58Z`

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-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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to a local unauthenticated vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     5.6.45
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.45, 5.7.27, 8.0.17 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.44 and prior, 5.7 through 5.7.26 and 8.0 through 8.0.16.

Vulnerability Insight
Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.26 / 8.0 <= 8.0.16 Security Update (.. ↪..`
OID:1.3.6.1.4.1.25623.1.0.143032
Version used: `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 <= 5.7.41, 8.x <= 8.0.32 Security Update (cpujul2023) - Windows

... continues on next page ...

... continued from previous page ...

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

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

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.42
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.42, 8.0.33 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.41 and prior and 8.x through 8.0.32.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.32 Security Update (cpujul2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149979
Version used: 2023-07-20T05:05:18Z

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-2023-22007
url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL
advisory-id: cpujul2023
cert-bund: WID-SEC-2023-1794
dfn-cert: DFN-CERT-2023-1642

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.

Quality of Detection: 80

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

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

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

Affected Software/OS
Oracle MySQL Server versions 5.5.47 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: 2023-11-03T05:05:46Z

Product Detection Result
Product: cpe:/a: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-2016-0649
cve: CVE-2016-0650
cve: CVE-2016-0644
cve: CVE-2016-0646
cve: CVE-2016-0640
cve: CVE-2016-0641
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0750
cert-bund: CB-K16/0646
cert-bund: CB-K16/0597
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0903
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0803
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0644

Medium (CVSS: 6.1)
NVT: Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows

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

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

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.41
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to version 5.7.41 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.7.40 Security Update (cpujan2023) - Windows`
OID:1.3.6.1.4.1.25623.1.0.149168
Version used: `2023-01-20T10:11:50Z`

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

References
`cve: CVE-2023-21840`
`url: https://www.oracle.com/security-alerts/cpujan2023.html#AppendixMSQL`
`advisory-id: cpujan2023`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0126`
`dfn-cert: DFN-CERT-2023-0105`

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.5.45 / 5.6 <= 5.6.26 Security Update (cpujan2016) - Windows

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

Summary
Oracle MySQL Server is prone to a vulnerability in a third party library.

Quality of Detection: 80

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
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`
`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 <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpuapr2016v3) - 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 unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote users to affect confidentiality, integrity, and availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.11.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.807924
Version used: 2023-11-03T05:05:46Z

Product Detection Result
Product: cpe:/a:mysql:mysql:5.5.20-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

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-0648
cve: CVE-2016-0642
cve: CVE-2016-0643
cve: CVE-2016-2047
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1129
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0750
cert-bund: CB-K16/0646
cert-bund: CB-K16/0597
cert-bund: CB-K16/0493
cert-bund: CB-K16/0133
dfn-cert: DFN-CERT-2016-1204
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0903
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0803
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0143
```

Medium (CVSS: 5.9)
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.

Quality of Detection: 80

Vulnerability Detection Result

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

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation of this vulnerability will allow remote attackers to 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: `2023-07-20T05:05:18Z`

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-2018-2761`
`cve: CVE-2018-2771`
`cve: CVE-2018-2781`
`cve: CVE-2018-2773`
`cve: CVE-2018-2817`
`cve: CVE-2018-2813`
`cve: CVE-2018-2755`
`cve: CVE-2018-2819`
`cve: CVE-2018-2818`
`url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: CB-K18/0608`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-1265
dfn-cert: DFN-CERT-2018-0913
dfn-cert: DFN-CERT-2018-0723

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.42 / 5.7 <= 5.7.24 / 8.0 <= 8.0.13 Security Update (cpuapr2019) - Windows

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

Summary
Oracle MySQL Server is prone to a vulnerability in the libmysqld subcomponent.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.43
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.43, 5.7.25, 8.0.14 or later.

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

... 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-2018-3123
url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
advisory-id: cpuapr2019
cert-bund: WID-SEC-2023-1594
cert-bund: CB-K19/0319
dfn-cert: DFN-CERT-2019-0775

Medium (CVSS: 5.9)
NVT: Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (cpuapr2019) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.43 / 5.7 <= 5.7.25 / 8.0 <= 8.0.15 Security Update (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.142403
Version used: `2022-03-28T03:06:01Z`

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

References
`cve: CVE-2019-1559`
`cve: CVE-2019-2683`
`cve: CVE-2019-2627`
`cve: CVE-2019-2614`
`url: https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL`
`advisory-id: cpuapr2019`
`cert-bund: WID-SEC-2023-2946`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: WID-SEC-2022-0462`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K19/0911`
`cert-bund: CB-K19/0639`
`cert-bund: CB-K19/0623`
`cert-bund: CB-K19/0622`
`cert-bund: CB-K19/0620`
`cert-bund: CB-K19/0619`
`cert-bund: CB-K19/0615`
`cert-bund: CB-K19/0332`
`cert-bund: CB-K19/0320`
`cert-bund: CB-K19/0319`
`cert-bund: CB-K19/0173`
`dfn-cert: DFN-CERT-2020-2620`
`dfn-cert: DFN-CERT-2020-2189`
`dfn-cert: DFN-CERT-2020-2180`
`dfn-cert: DFN-CERT-2020-0092`
`dfn-cert: DFN-CERT-2020-0048`
`dfn-cert: DFN-CERT-2019-2625`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2300
dfn-cert: DFN-CERT-2019-2274
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-2008
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1713
dfn-cert: DFN-CERT-2019-1683
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0968
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412
```

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.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.3
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack.

Solution:
Solution type: VendorFix
Upgrade to version Oracle MySQL Server 5.7.3 or later.

Affected Software/OS
Oracle MySQL Server 5.7.2 and earlier on Windows.

Vulnerability Insight
The flaw exists due to improper validation of MySQL client library when establishing a secure connection to a MySQL server using the –ssl option.

Vulnerability Detection Method
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

... continues on next page ...

... continued from previous page ...

```
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: 5.7)
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.

Quality of Detection: 80

Vulnerability Detection Result

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

Impact

Successful exploitation will allow an authenticated remote attacker to cause a denial of service.

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

Affected Software/OS

Oracle MySQL Server 5.5.42 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)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.805172
Version used: 2023-07-25T05:05:58Z

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-2015-2571
cve: CVE-2015-0505
cve: CVE-2015-0501
cve: CVE-2015-0499
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74095
url: http://www.securityfocus.com/bid/74112
url: http://www.securityfocus.com/bid/74070
url: http://www.securityfocus.com/bid/74115
cert-bund: WID-SEC-2023-2068
cert-bund: CB-K15/1546
cert-bund: CB-K15/1518
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720
cert-bund: CB-K15/0531
dfn-cert: DFN-CERT-2015-1623
dfn-cert: DFN-CERT-2015-1604
dfn-cert: DFN-CERT-2015-1272
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1105
dfn-cert: DFN-CERT-2015-1096
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0551

Medium (CVSS: 5.6)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows

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

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation of this vulnerability will allow remote to have an impact on availability, confidentiality and integrity.

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

Affected Software/OS
Oracle MySQL version 5.5.53 and earlier, 5.6.34 and earlier, 5.7.16 and earlier on Windows

Vulnerability Insight
Multiple flaws exist due to: multiple unspecified errors in sub components 'Error Handling', 'Logging', 'MyISAM', 'Packaging', 'Optimizer', 'DML' and 'DDL'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.809865
Version used: `2023-07-14T16:09:27Z`

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

References
```
cve: CVE-2017-3238
cve: CVE-2017-3318
cve: CVE-2017-3291
cve: CVE-2017-3317
cve: CVE-2017-3258
```

... continues on next page ...

... continued from previous page ...

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
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: 5.6)
NVT: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Windows

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

Summary
Oracle MySQL Server is prone to a unspecified vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

... continues on next page ...

... continued from previous page ...

Fixed version: 5.7.43
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.43, 8.0.34 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.42 and prior and 8.x through 8.0.33.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.42, 8.x <= 8.0.33 Security Update (cpujul2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149981
Version used: 2023-07-20T05:05:18Z

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-2023-22053
url: https://www.oracle.com/security-alerts/cpujul2023.html#AppendixMSQL
advisory-id: cpujul2023
cert-bund: WID-SEC-2023-1794
dfn-cert: DFN-CERT-2023-1642

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

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

Impact
Successful exploitation will allow local users to affect availability.

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

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior.

Vulnerability Insight
Unspecified error exists in the 'MySQL Server' component via unknown vectors related to 'Optimizer'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 Security Update (cpuapr2016v3) - Windows
OID:1.3.6.1.4.1.25623.1.0.807922
Version used: 2022-08-31T10:10:28Z

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

References
cve: CVE-2016-0651
url: https://www.oracle.com/security-alerts/cpuapr2016v3.html#AppendixMSQL
advisory-id: cpuapr2016v3
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0597
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0644

Medium (CVSS: 5.5)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpujan2022) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.37
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.36 and prior and 8.0 through 8.0.27.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (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

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2022-21245
cve: CVE-2021-22947
url: https://www.oracle.com/security-alerts/cpujan2022.html#AppendixMSQL
advisory-id: cpujan2022
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: CB-K22/0316
cert-bund: CB-K22/0077
cert-bund: CB-K22/0062
cert-bund: CB-K22/0030
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
dfn-cert: DFN-CERT-2022-2376
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2047
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: 5.3)
NVT: Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Windows

Product detection result

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

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to multiple vulnerabilities in OpenSSL.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     5.6.47
Installation
path / port:       3306/tcp
```

Solution:
Solution type: VendorFix
Update to version 5.6.47, 5.7.27 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.46 and prior and 5.7 through 5.7.26.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Server <= 5.6.46 / 5.7 <= 5.7.26 Security Update (cpuapr2020) - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143735
Version used: `2021-08-16T09:00:57Z`

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

References
```
cve: CVE-2019-1547
cve: CVE-2019-1549
cve: CVE-2019-1552
cve: CVE-2019-1563
url: https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixMSQL
advisory-id: cpuapr2020
cert-bund: WID-SEC-2023-3081
cert-bund: WID-SEC-2023-1762
cert-bund: WID-SEC-2023-1049
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
```

... continues on next page ...

... continued from previous page ...

```
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-2023-2709
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1900
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1559
```

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

Product detection result

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

Summary

Oracle MySQL is prone to vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.5.20
Fixed version: Apply the patch

Impact
Successful exploitation of this vulnerability will allow remote attackers to partially access data, partially modify data, and partially deny service.

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

Affected Software/OS
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, on Windows

Vulnerability Insight
The flaw exists due to an error in the Client programs component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows
OID:1.3.6.1.4.1.25623.1.0.811434
Version used: 2023-07-14T16:09:27Z

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

References
cve: CVE-2017-3636
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
↪#AppendixMSQL
url: http://www.securityfocus.com/bid/99736
cert-bund: CB-K18/0224
cert-bund: CB-K17/1870
cert-bund: CB-K17/1604
cert-bund: CB-K17/1453
cert-bund: CB-K17/1401
cert-bund: CB-K17/1239
cert-bund: CB-K17/1205
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1956
dfn-cert: DFN-CERT-2017-1675
dfn-cert: DFN-CERT-2017-1519

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243

Medium (CVSS: 5.3)
NVT: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Windows

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

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.40, 8.0.31 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.30.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.39 / 8.0 <= 8.0.30 Security Update (cpuoct2022) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.118388
Version used: 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

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-2097
cve: CVE-2022-21617
cve: CVE-2022-21608
url: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixMSQL
advisory-id: cpuoct2022
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1777
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1146
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1065
cert-bund: WID-SEC-2022-0561
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2491
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1058
dfn-cert: DFN-CERT-2023-0509
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2315
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1536
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1515
dfn-cert: DFN-CERT-2022-1497
```

Medium (CVSS: 5.3)
NVT: Oracle Mysql Security Updates (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)
```

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to a security bypass vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation of this vulnerability will allow remote attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack. This may lead to other attacks also.

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

Affected Software/OS
Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier on Windows

Vulnerability Insight
The flaw exists due to an incorrect implementation or enforcement of 'ssl-mode=REQUIRED' in MySQL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows`
OID:1.3.6.1.4.1.25623.1.0.810884
Version used: `2023-07-25T05:05:58Z`

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-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
```

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.46
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.46, 5.7.28 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)

... continues on next page ...

... continued from previous page ...

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: 5.0)
NVT: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)

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

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL 5.5.30 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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-03 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803725
Version used: 2023-07-27T05:05:08Z

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-2013-3801
cve: CVE-2013-3805
cve: CVE-2013-3794
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61222
url: http://www.securityfocus.com/bid/61256
url: http://www.securityfocus.com/bid/61269
cert-bund: CB-K13/0919
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 5.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)

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

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: Apply the patch
Installation

... continues on next page ...

... continued from previous page ...

path / port: 3306/tcp

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: 2023-07-25T05:05:58Z

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-2015-2573
cve: CVE-2015-2568
cve: CVE-2015-0441
cve: CVE-2015-0433
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74078
url: http://www.securityfocus.com/bid/74073
url: http://www.securityfocus.com/bid/74103
url: http://www.securityfocus.com/bid/74089
cert-bund: WID-SEC-2023-2068
cert-bund: CB-K15/1546
cert-bund: CB-K15/1202
cert-bund: CB-K15/1193
cert-bund: CB-K15/1045
cert-bund: CB-K15/1042
cert-bund: CB-K15/0964
cert-bund: CB-K15/0720

... continues on next page ...

... continued from previous page ...

```
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 <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Windows

Product detection result

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

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.31
Installation
path / port:       3306/tcp
```

Solution:

Solution type: VendorFix

Update to version 5.7.31, 8.0.18 or later.

Affected Software/OS

Oracle MySQL Server version 5.7.30 and prior and 8.0 through 8.0.17.

Vulnerability Detection Method

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

Details: `Oracle MySQL Server <= 5.7.30 / 8.0 <= 8.0.17 Security Update (cpuapr2021) - Wi.
↪..`

OID:1.3.6.1.4.1.25623.1.0.145804

Version used: `2021-08-26T13:01:12Z`

Product Detection Result

... continues on next page ...

... continued from previous page ...

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

References
cve: CVE-2021-2160
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2021-0821

Medium (CVSS: 4.9)
NVT: Oracle MySQL Security Update (cpujul2018 - 04) - Windows

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

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

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

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

Affected Software/OS
Oracle MySQL version 5.5.60 and earlier.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws exist due to an error in the 'Server: Security: Privileges' component of MySQL Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Security Update (cpujul2018 - 04) - Windows`
OID:1.3.6.1.4.1.25623.1.0.813710
Version used: `2022-08-22T10:11:10Z`

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

References
`cve: CVE-2018-3063`
`url: https://www.oracle.com/security-alerts/cpujul2018.html#AppendixMSQL`
`advisory-id: cpujul2018`
`cert-bund: WID-SEC-2023-1594`
`cert-bund: CB-K18/0795`
`dfn-cert: DFN-CERT-2019-1614`
`dfn-cert: DFN-CERT-2019-1588`
`dfn-cert: DFN-CERT-2019-1152`
`dfn-cert: DFN-CERT-2019-1047`
`dfn-cert: DFN-CERT-2019-0484`
`dfn-cert: DFN-CERT-2018-1649`
`dfn-cert: DFN-CERT-2018-1402`

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.30 / 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.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 5.5.20`

... continues on next page ...

... continued from previous page ...

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: WID-SEC-2023-0067
cert-bund: CB-K21/0062
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0810
dfn-cert: DFN-CERT-2021-0131

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (cpujan2021) - Windows

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

... continues on next page ...

... continued from previous page ...

↪25623.1.0.100152)

Summary
Oracle MySQL Server is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.51
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.51, 5.7.33, 8.0.23 or later.

Affected Software/OS
Oracle MySQL Server versions 5.6.50 and prior, 5.7 through 5.7.32 and 8.0 through 8.0.22.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.6.50 / 5.7 <= 5.7.32 / 8.0 <= 8.0.22 Security Update (.
↪..
OID:1.3.6.1.4.1.25623.1.0.145224
Version used: 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: WID-SEC-2023-0067
cert-bund: CB-K21/0062
dfn-cert: DFN-CERT-2021-2155
dfn-cert: DFN-CERT-2021-0131

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server <= 5.7.33 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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.34
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.34 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.33 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.33 Security Update (cpuapr2021) - Windows
OID:1.3.6.1.4.1.25623.1.0.145802
Version used: 2021-08-26T13:01:12Z

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

References
cve: CVE-2021-2154
url: https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixMSQL
advisory-id: cpuapr2021
cert-bund: WID-SEC-2023-0065
cert-bund: CB-K21/0421
dfn-cert: DFN-CERT-2022-1241
dfn-cert: DFN-CERT-2022-0933

. . . continues on next page . . .

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0666
dfn-cert: DFN-CERT-2021-1660
dfn-cert: DFN-CERT-2021-0984
dfn-cert: DFN-CERT-2021-0821

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

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

Affected Software/OS
Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows

Vulnerability Insight
Unspecified error in the MySQL Server component via unknown vectors related to Replication.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 .
↪..
OID:1.3.6.1.4.1.25623.1.0.804034
Version used: 2023-07-27T05:05:08Z

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: 4.6)
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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.40
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.40, 8.0.30 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.39 and prior and 8.0 through 8.0.29.

... 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 <= 5.7.39 / 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-2023-2031`
`cert-bund: WID-SEC-2022-1776`
`dfn-cert: DFN-CERT-2022-2306`

Medium (CVSS: 4.6)
NVT: Oracle MySQL Server <= 5.7.36 / 8.0 <= 8.0.27 Security Update (cpuoct2022) - Windows

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

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

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version: 5.7.37`
`Installation`
`path / port: 3306/tcp`

Solution:
Solution type: VendorFix
Update to version 5.7.37, 8.0.28 or later.

... 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 (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-2023-0504`
`dfn-cert: DFN-CERT-2022-2306`

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.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version: 5.7.40`
`Installation`
`path / port: 3306/tcp`

Solution:

... continues on next page ...

... continued from previous page ...

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-2023-2031`
`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.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 5.5.20`
`Fixed version: 5.5.30`

... continues on next page ...

... continued from previous page ...

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: 4.4)
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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

... continues on next page ...

... continued from previous page ...

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

Impact
Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.

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

Affected Software/OS
Oracle MySQL version 5.5.53 and earlier on Windows

Vulnerability Insight
The flaw exists due to an unspecified error in sub component 'Server: Charsets'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows
OID:1.3.6.1.4.1.25623.1.0.809869
Version used: 2023-07-25T05:05:58Z

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-2017-3243
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/95538
cert-bund: CB-K18/0224
cert-bund: CB-K17/1298
cert-bund: CB-K17/0098
dfn-cert: DFN-CERT-2018-0242
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-0090

Medium (CVSS: 4.3)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15

Product detection result

... continues on next page ...

... continued from previous page ...

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

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an authenticated remote attacker to affect confidentiality via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier on Windows

Vulnerability Insight
Unspecified errors exist in the MySQL Server component via unknown vectors related to Server : Pluggable Auth and Server : Security : Privileges.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15
OID:1.3.6.1.4.1.25623.1.0.805930
Version used: 2023-07-25T05:05:58Z

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-2015-4737
cve: CVE-2015-2620

... continues on next page ...

... continued from previous page ...

```
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.

Quality of Detection: 80

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

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

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

Affected Software/OS
Oracle MySQL version 5.5.56 and earlier, 5.6.36 and earlier, 5.7.18 and earlier, on Windows

Vulnerability Insight
Multiple flaws exist due to

... continues on next page ...

... continued from previous page ...

- A flaw in the Client mysqldump component.
- A flaw in the Server: DDL component.
- A flaw in the C API component.
- A flaw in the Connector/C component.
- A flaw in the Server: Charsets component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811432
Version used: `2023-03-24T10:19:42Z`

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

References
`cve: CVE-2017-3651`
`cve: CVE-2017-3653`
`cve: CVE-2017-3652`
`cve: CVE-2017-3635`
`cve: CVE-2017-3648`
`cve: CVE-2017-3641`
`url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html`
`↪#AppendixMSQL`
`url: http://www.securityfocus.com/bid/99802`
`url: http://www.securityfocus.com/bid/99810`
`url: http://www.securityfocus.com/bid/99805`
`url: http://www.securityfocus.com/bid/99730`
`url: http://www.securityfocus.com/bid/99789`
`url: http://www.securityfocus.com/bid/99767`
`cert-bund: CB-K18/0224`
`cert-bund: CB-K17/1870`
`cert-bund: CB-K17/1732`
`cert-bund: CB-K17/1604`
`cert-bund: CB-K17/1453`
`cert-bund: CB-K17/1401`
`cert-bund: CB-K17/1298`
`cert-bund: CB-K17/1239`
`cert-bund: CB-K17/1205`
`dfn-cert: DFN-CERT-2018-1276`
`dfn-cert: DFN-CERT-2018-0242`
`dfn-cert: DFN-CERT-2017-1956`
`dfn-cert: DFN-CERT-2017-1806`
`dfn-cert: DFN-CERT-2017-1675`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-1519
dfn-cert: DFN-CERT-2017-1465
dfn-cert: DFN-CERT-2017-1341
dfn-cert: DFN-CERT-2017-1282
dfn-cert: DFN-CERT-2017-1243

Medium (CVSS: 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, 5.6.11 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Full Text Search and Server Optimizer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: MySQL Unspecified vulnerabilities-01 July-2013 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803723
Version used: 2023-07-27T05:05:08Z

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-2013-3804
cve: CVE-2013-3802
url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
url: http://www.securityfocus.com/bid/61244
url: http://www.securityfocus.com/bid/61260
cert-bund: CB-K13/1072
cert-bund: CB-K13/0620
dfn-cert: DFN-CERT-2013-2099
dfn-cert: DFN-CERT-2013-1599
dfn-cert: DFN-CERT-2013-1553
dfn-cert: DFN-CERT-2013-1478

Medium (CVSS: 4.0)
NVT: 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an authenticated remote attacker to cause denial-of-service attack.

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-25T05:05:58Z`

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-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-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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 5.5.20-log`
`Vulnerable range: 5.5 - 5.5.37`

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.5.37 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to ENARC and SROPTZR.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 July14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804723
Version used: `2023-07-26T05:05:09Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-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`

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

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

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

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

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Server:InnoDB:DDL:Foreign Key

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

... continues on next page ...

... continued from previous page ...

Details: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805133
Version used: 2023-07-25T05:05:58Z

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-2015-0432
url: http://secunia.com/advisories/62525
url: http://www.securityfocus.com/bid/72217
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/1193
cert-bund: CB-K15/0964
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0073
dfn-cert: DFN-CERT-2015-1264
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0074

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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

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

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805135
Version used: `2023-07-25T05:05:58Z`

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-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 - 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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to InnoDB, Optimizer, Error Handling, and some unknown vectors.

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: `2023-07-26T05:05:09Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.5.20-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`

... continues on next page ...

... continued from previous page ...

```
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: MySQL Unspecified vulnerability-06 July-2013 (Windows)

Product detection result

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

Summary
MySQL is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL 5.5.31 and earlier on Windows.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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-2013-3783`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61210`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
Oracle MySQL versions 5.1.51 through 5.1.70, 5.5.10 through 5.5.32, and 5.6.x through 5.6.12 on Windows.

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: `2023-07-27T05:05:08Z`

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-2013-3839`
`url: http://secunia.com/advisories/55327`
`url: http://www.securityfocus.com/bid/63109`
`url: http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0840`
`cert-bund: CB-K13/0806`
`cert-bund: CB-K13/0789`
`dfn-cert: DFN-CERT-2014-0190`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1846`
`dfn-cert: DFN-CERT-2013-1815`
`dfn-cert: DFN-CERT-2013-1795`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Multiple Vulnerabilities-03 Nov12 (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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information, manipulate certain data.

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

Affected Software/OS
Oracle MySQL version 5.1.x to 5.1.63 and Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
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: 2023-07-25T05:05:58Z

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-2012-3173
cve: CVE-2012-3167
cve: CVE-2012-3166
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56018

... continues on next page ...

... continued from previous page ...

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 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to Optimizer, InnoDB, and Locking.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804076
Version used: 2023-07-26T05:05:09Z

... 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-2014-0386
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 Server 5.5 <= 5.5.30 / 5.6 <= 5.6.10 Security Update (cpuapr2013) - Windows

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

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20

... continues on next page ...

... continued from previous page ...

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
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

... 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 unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.30
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.5.30 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.29.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.29 Security Update (cpuapr2013) - Windows
OID:1.3.6.1.4.1.25623.1.0.117215
Version used: 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 Server <= 5.5.46 Security Update (cpujan2016) - 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 an unspecified vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

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

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

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133
cert-bund: CB-K16/0094
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0994
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2016-0143
dfn-cert: DFN-CERT-2016-0104
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.5.35 and earlier and 5.6.15 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 Partition, Replication and XML subcomponent.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804574
Version used: `2023-07-26T05:05:09Z`

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

References
`cve: CVE-2014-0384`
`cve: CVE-2014-2419`
`cve: CVE-2014-2438`
`url: http://secunia.com/advisories/57940`
`url: http://www.securityfocus.com/bid/66835`
`url: http://www.securityfocus.com/bid/66846`
`url: http://www.securityfocus.com/bid/66880`
`url: http://www.scaprepo.com/view.jsp?id=oval:org.secpod.oval:def:701638`
`url: http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0464`
`cert-bund: CB-K14/0452`
`dfn-cert: DFN-CERT-2014-0742`
`dfn-cert: DFN-CERT-2014-0477`
`dfn-cert: DFN-CERT-2014-0459`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-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.

Quality of Detection: 80

... 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 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: 2023-07-25T05:05:58Z

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-2015-4913
cve: CVE-2015-4830
cve: CVE-2015-4826
cve: CVE-2015-4815
cve: CVE-2015-4807
cve: CVE-2015-4802
cve: CVE-2015-4792
cve: CVE-2015-4870
cve: CVE-2015-4861
cve: CVE-2015-4858
cve: CVE-2015-4836
url: http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/77153
url: http://www.securityfocus.com/bid/77228
url: http://www.securityfocus.com/bid/77237
url: http://www.securityfocus.com/bid/77222
url: http://www.securityfocus.com/bid/77205
url: http://www.securityfocus.com/bid/77165
url: http://www.securityfocus.com/bid/77171
url: http://www.securityfocus.com/bid/77208
url: http://www.securityfocus.com/bid/77137
url: http://www.securityfocus.com/bid/77145
url: http://www.securityfocus.com/bid/77190
cert-bund: CB-K16/1122
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K15/1844
cert-bund: CB-K15/1600
cert-bund: CB-K15/1554
dfn-cert: DFN-CERT-2016-1192
dfn-cert: DFN-CERT-2016-0845
dfn-cert: DFN-CERT-2016-0695
dfn-cert: DFN-CERT-2016-0532
dfn-cert: DFN-CERT-2016-0266
dfn-cert: DFN-CERT-2016-0265
dfn-cert: DFN-CERT-2015-1946
dfn-cert: DFN-CERT-2015-1692
dfn-cert: DFN-CERT-2015-1638
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL 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.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
```

... continues on next page ...

... continued from previous page ...

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

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

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

Affected Software/OS
Oracle MySQL Server versions 5.5.46 and prior and 5.6 through 5.6.27.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.46 / 5.6 <= 5.6.27 Security Update (cpujan2016) - Wi.
↪..
OID:1.3.6.1.4.1.25623.1.0.806877
Version used: 2022-04-13T13:17:10Z

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

References
cve: CVE-2016-0596
url: https://www.oracle.com/security-alerts/cpujan2016.html#AppendixMSQL
url: http://www.securityfocus.com/bid/81176
url: http://www.securityfocus.com/bid/81198
url: http://www.securityfocus.com/bid/81130
advisory-id: cpujan2016
cert-bund: CB-K16/1122
cert-bund: CB-K16/0936
cert-bund: CB-K16/0791
cert-bund: CB-K16/0646
cert-bund: CB-K16/0493
cert-bund: CB-K16/0246
cert-bund: CB-K16/0245
cert-bund: CB-K16/0133

... continues on next page ...

... continued from previous page ...

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: MySQL Server Component Partition Unspecified Vulnerability

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

Summary
MySQL is prone to an unspecified vulnerability.

Quality of Detection: 80

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
OID:1.3.6.1.4.1.25623.1.0.803801

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-27T05:05:08Z

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-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: 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote authenticated users to affect availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier and 5.6.10 on Windows.

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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-2013-3808`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61227`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

Medium (CVSS: 4.0)
NVT: MySQL Unspecified 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)`

Summary
MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow remote authenticated users to affect integrity and availability via unknown vectors and cause denial of service.

Solution:

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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-2013-3812`
`cve: CVE-2013-3809`
`cve: CVE-2013-3793`
`url: http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html`
`url: http://www.securityfocus.com/bid/61249`
`url: http://www.securityfocus.com/bid/61264`
`url: http://www.securityfocus.com/bid/61272`
`cert-bund: CB-K13/1072`
`cert-bund: CB-K13/0620`
`dfn-cert: DFN-CERT-2013-2099`
`dfn-cert: DFN-CERT-2013-1599`
`dfn-cert: DFN-CERT-2013-1553`
`dfn-cert: DFN-CERT-2013-1478`

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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 5.5.20
Fixed version:     5.5.23
Installation
path / port:       3306/tcp
```

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

Solution:
Solution type: VendorFix
Update to version 5.1.63, 5.5.23 or later.

Affected Software/OS
Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.22.

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`
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 <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - Windows

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

Summary
Oracle MySQL Server is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.24
Installation
path / port: 3306/tcp

Impact
The flaws allow remote authenticated users to affect availability via unknown vectors related to the 'Server Optimizer' and 'GIS Extension' package / privilege.

Solution:
Solution type: VendorFix
Update to version 5.1.63, 5.5.24 or later.

Affected Software/OS
Oracle MySQL Server 5.1.62 and prior and 5.4.x through 5.5.23.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.1.62 / 5.4.x <= 5.5.23 Security Update (cpujul2012) - .
↪..
OID:1.3.6.1.4.1.25623.1.0.117265
Version used: 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

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2012-1734
cve: CVE-2012-2749
url: https://www.oracle.com/security-alerts/cpujul2012.html#AppendixMSQL
advisory-id: cpujul2012
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2012-2118
dfn-cert: DFN-CERT-2012-1389
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server <= 5.5.38 Security Update (cpuoct2014) - Windows

Product detection result

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

Summary

Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.39
Installation
path / port:       3306/tcp
```

Impact

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

Solution:

Solution type: VendorFix

Update to version 5.5.39 or later.

Affected Software/OS

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

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.5.38 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 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.

Quality of Detection: 80

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

... continues on next page ...

... continued from previous page ...

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: `2023-07-27T05:05:08Z`

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-2013-5891`
`url: http://secunia.com/advisories/56491`
`url: http://www.securityfocus.com/bid/64891`
`url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html`
`cert-bund: CB-K14/0710`
`cert-bund: CB-K14/0187`
`cert-bund: CB-K14/0082`
`cert-bund: CB-K14/0074`
`cert-bund: CB-K14/0055`
`dfn-cert: DFN-CERT-2014-0742`
`dfn-cert: DFN-CERT-2014-0190`
`dfn-cert: DFN-CERT-2014-0085`
`dfn-cert: DFN-CERT-2014-0074`
`dfn-cert: DFN-CERT-2014-0048`

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an authenticated remote attacker to affect availability via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server 5.5.44 and earlier on windows

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805771
Version used: 2023-07-25T05:05:58Z

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

. . . continues on next page . . .

... continued from previous page ...

```
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
```

[return to 10.0.2.4]

2.2.11 Medium 8181/tcp

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

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

Quality of Detection: 99

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)                | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)              | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 04A9972F
signature algorithm                | sha256WithRSAEncryption
```

... continues on next page ...

... continued from previous page ...

subject	CN=localhost,OU=GlassFish,O=Oracle Corporation ↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)	None
valid from	2013-05-15 05:33:38 UTC
valid until	2023-05-13 05:33:38 UTC

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

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

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

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

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

Quality of Detection: 99

Vulnerability Detection Result
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:

fingerprint (SHA-1)	4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)	AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD ↪5B23381002A885F556
issued by	CN=localhost,OU=GlassFish,O=Oracle Corporation ↪,L=Santa Clara,ST=California,C=US
public key algorithm	RSA
public key size (bits)	2048
serial	04A9972F
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost,OU=GlassFish,O=Oracle Corporation ↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)	None
valid from	2013-05-15 05:33:38 UTC

... continues on next page ...

... continued from previous page ...

valid until	2023-05-13 05:33:38 UTC

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

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

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

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

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

Quality of Detection: 70

Vulnerability Detection Result
The following indicates that the remote SSL/TLS service is affected:

Protocol Version	Successful re-done SSL/TLS handshakes (Renegotiation) over an existing / already established SSL/TLS connection
TLSv1.0	10
TLSv1.1	10
TLSv1.2	10

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

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

References
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

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.

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

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: `2023-10-20T16:09:12Z`

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
```

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2014-1414

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2011-1706

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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

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

Quality of Detection: 80

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

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

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

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

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.0.2.4]

2.2.12 Medium 135/tcp

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

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

Quality of Detection: 80

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49152]
Port: 49153/tcp
      UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49153]
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49153]
      Annotation: Event log TCPIP
Port: 49154/tcp
      UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      Annotation: IKE/Authip API
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49154]
      Annotation: Impl friendly name
```

. . . continues on next page . . .

... continued from previous page ...

```
Port: 49177/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:10.0.2.4[49177]
Port: 49178/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49178]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49202/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49202]
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:10.0.2.4[49202]
      Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

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

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

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

[return to 10.0.2.4]

2.2.13 Medium 4848/tcp

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

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection: 99

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)                | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)              | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 04A9972F
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)    | None
valid from                         | 2013-05-15 05:33:38 UTC
valid until                        | 2023-05-13 05:33:38 UTC
```

Impact

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

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection: 99

Vulnerability Detection Result

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)                | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)              | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                          | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 04A9972F
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN)    | None
valid from                         | 2013-05-15 05:33:38 UTC
valid until                        | 2023-05-13 05:33:38 UTC
```

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

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: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

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

Quality of Detection: 70

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: WID-SEC-2023-1435`

... continues on next page ...

... continued from previous page ...

```
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: 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.

Quality of Detection: 98

Vulnerability Detection Result

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

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

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

... continues on next page ...

... continued from previous page ...

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

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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

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

Quality of Detection: 80

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

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

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.0.2.4]

2.2.14 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows

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

Summary
OpenSSH is prone to a user enumeration vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: 7.8`
`Installation`
`path / port: 22/tcp`

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.8 User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2023-07-20T05:05:18Z`

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

References
`cve: CVE-2018-15473`
`url: https://0day.city/cve-2018-15473.html`
`url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d`
`↪1e0`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K18/1031`
`cert-bund: CB-K18/0873`
`dfn-cert: DFN-CERT-2021-2178`
`dfn-cert: DFN-CERT-2020-2189`
`dfn-cert: DFN-CERT-2020-0228`
`dfn-cert: DFN-CERT-2019-2046`
`dfn-cert: DFN-CERT-2019-0857`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2259`
`dfn-cert: DFN-CERT-2018-2191`
`dfn-cert: DFN-CERT-2018-1806`
`dfn-cert: DFN-CERT-2018-1696`

Medium (CVSS: 5.3)
NVT: OpenSSH '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.

Quality of Detection: 80

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: None`
`Installation path / port: 22/tcp`

Impact
Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

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

Affected Software/OS
OpenSSH version 5.9 through 7.8.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813887
Version used: `2021-05-28T07:06:21Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`

. . . continues on next page . . .

... continued from previous page ...

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 '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.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 7.1
Fixed version: 7.6
Installation
path / port: 22/tcp

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

Solution:
Solution type: VendorFix
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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: 2023-07-14T16:09:27Z

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

References
cve: CVE-2017-15906
url: https://www.openssh.com/txt/release-7.6
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

[return to 10.0.2.4]

2.2.15 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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

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

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

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2021-12-01T13:10:37Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
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

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

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

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

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

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

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

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

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

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2023-10-20T16:09:12Z

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

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

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

Quality of Detection: 80

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=vagrant-2008R2
Signature Algorithm:  sha1WithRSAEncryption
```

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

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

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

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

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

[return to 10.0.2.4]

2.2.16 Medium 8383/tcp

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.

Quality of Detection: 80

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00F59CEF71E6DB72A5:1.2.840.113549.1.9.1=#737570706F7274406465736B746F70,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleasanton,ST=CA,C=US (Server certificate)

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
OID:1.3.6.1.4.1.25623.1.0.150710

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 99

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.

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

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

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

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

Quality of Detection: 98

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

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

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more 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: `2023-10-20T16:09:12Z`

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`

. . . continues on next page . . .

... continued from previous page ...

```
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
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
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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

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

Quality of Detection: 80

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#737570706F7274406465736B746F7063656E
↪7472616C2E636F6D,CN=Desktop Central,OU=ManageEngine,O=Zoho Corporation,L=Pleas
↪anton,ST=CA,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

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

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered 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.

... continues on next page ...

... continued from previous page ...

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

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

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

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

Quality of Detection: 80

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

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

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

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

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2023-07-21T05:05:22Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 10.0.2.4]

2.2.17 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.2.4]

2.2.18 Low 9200/tcp

Low (CVSS: 3.1)
NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.13
Installation
path / port:       /
```

Impact
This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.13, 7.9.2 or later.

Affected Software/OS
Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.

... 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 10.0.2.4]

2.2.19 Low 3306/tcp

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.11 Security Update (cpu-jul2016) - Windows

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation 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`
`dfn-cert: DFN-CERT-2016-1192`
`dfn-cert: DFN-CERT-2016-1169`

Low (CVSS: 3.7)
NVT: Oracle MySQL Server <= 5.5.48 / 5.6 <= 5.6.29 / 5.7 <= 5.7.10 Security Update (cpujul2016) - Windows

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

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact
Successful exploitation will allow a remote attacker to affect confidentiality via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server versions 5.5.48 and prior, 5.6 through 5.6.29 and 5.7 through 5.7.10.

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
```

... 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an authenticated remote attacker to cause denial of service attack.

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

Affected Software/OS
Oracle MySQL Server 5.5.42 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: 2023-07-25T05:05:58Z

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-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 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.

Quality of Detection: 80

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

Impact
Successful exploitation will allow an attacker to disclose potentially sensitive information and manipulate certain data.

Solution:
Solution type: VendorFix
Apply the patch from the linked references or upgrade to latest version.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Oracle MySQL version 5.5.x to 5.5.25 on Windows.

Vulnerability Insight
The flaw is due to unspecified error in MySQL server component vectors server.

Vulnerability Detection Method
Details: Oracle MySQL Server Multiple Vulnerabilities-05 Nov12 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803115
Version used: 2023-07-25T05:05:58Z

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-2012-3156
url: http://secunia.com/advisories/51008/
url: http://www.securityfocus.com/bid/56013
url: http://www.securelist.com/en/advisories/51008
url: http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
url: https://support.oracle.com/rs?type=doc&id=1475188.1

Low (CVSS: 3.5)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)

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

Summary
Oracle MySQL is prone to an unspecified vulnerability.

Quality of Detection: 80

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

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an authenticated remote attacker to affect integrity via unknown vectors.

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

Affected Software/OS
Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on windows

Vulnerability Insight
Unspecified error exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805770
Version used: `2023-07-25T05:05:58Z`

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-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: 3.3)
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)`

... continues on next page ...

... continued from previous page ...

Summary
Oracle MySQL is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: See reference
Installation
path / port: 3306/tcp

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

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

Affected Software/OS
Oracle MySQL version 5.5.60 and earlier, 5.6.40 and earlier, 5.7.22 and earlier.

Vulnerability Insight
Multiple flaws exist due to errors in 'Server: Security: Encryption', 'Server: Options', 'MyISAM', 'Client mysqldump' components of application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
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: WID-SEC-2023-1594

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0795
dfn-cert: DFN-CERT-2019-1614
dfn-cert: DFN-CERT-2019-1588
dfn-cert: DFN-CERT-2019-1152
dfn-cert: DFN-CERT-2019-1047
dfn-cert: DFN-CERT-2019-0484
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-1649
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1276
dfn-cert: DFN-CERT-2018-0913

Low (CVSS: 3.3)
NVT: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows

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

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

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.7.41
Installation
path / port: 3306/tcp

Solution:
Solution type: VendorFix
Update to version 5.7.41, 8.0.32 or later.

Affected Software/OS
Oracle MySQL Server version 5.7.40 and prior and 8.x through 8.0.31.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpuapr2023) - Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.149532
Version used: 2023-04-19T10:19:33Z

... 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-2023-21963
url: https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixMSQL
advisory-id: cpuapr2023
cert-bund: WID-SEC-2023-1033
dfn-cert: DFN-CERT-2023-0885

Low (CVSS: 2.8)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)

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

Summary
Oracle MySQL is prone to multiple unspecified vulnerabilities.

Quality of Detection: 80

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

Impact
Successful exploitation will allow attackers to manipulate certain data and cause a DoS (Denial of Service).

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

Affected Software/OS
Oracle MySQL version 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804077
Version used: 2023-07-27T05:05:09Z

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

References
cve: CVE-2014-0420
url: http://secunia.com/advisories/56491
url: http://www.securityfocus.com/bid/64888
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0710
cert-bund: CB-K14/0187
cert-bund: CB-K14/0082
cert-bund: CB-K14/0074
cert-bund: CB-K14/0055
dfn-cert: DFN-CERT-2014-0742
dfn-cert: DFN-CERT-2014-0190
dfn-cert: DFN-CERT-2014-0085
dfn-cert: DFN-CERT-2014-0074
dfn-cert: DFN-CERT-2014-0048

Low (CVSS: 2.7)
NVT: Oracle MySQL Server <= 5.6.44 / 5.7 <= 5.7.18 Security Update (cpujul2019) - Windows

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

Summary
Oracle MySQL Server is prone to an unspecified vulnerability.

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.6.45
Installation

... continues on next page ...

... continued from previous page ...

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)
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.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.5.20
Fixed version: 5.5.31
Installation
path / port: 3306/tcp

Impact
Successful exploitation will allow local users to affect availability.

Solution:
Solution type: VendorFix
Update to version 5.5.31, 5.6.10 or later.

Affected Software/OS
Oracle MySQL Server versions 5.5 through 5.5.30 and 5.6 through 5.6.9.

Vulnerability Insight
An unspecified error exists in the MySQL Server component via unknown vectors related to Server Partition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Oracle MySQL Server 5.5 <= 5.5.30 / 5.6 <= 5.6.9 Security Update (cpuapr2013) -.
↪..
OID:1.3.6.1.4.1.25623.1.0.809813
Version used: 2022-04-25T14:50:49Z

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

References
cve: CVE-2013-1502
url: https://www.oracle.com/security-alerts/cpuapr2013.html#AppendixMSQL
url: http://www.securityfocus.com/bid/59239
advisory-id: cpuapr2013
dfn-cert: DFN-CERT-2013-0882
dfn-cert: DFN-CERT-2013-0798

[return to 10.0.2.4]

2.2.20 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 226379
Packet 2: 226491
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-08-01T13:29:10Z`

References
```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 10.0.2.4]

2.2.21 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 10.0.2.4]

2.3 10.0.2.2

Host scan start	Mon Dec 11 18:10:04 2023 UTC
Host scan end	Mon Dec 11 18:21:13 2023 UTC

Service (Port)	Threat Level
135/tcp	Medium

2.3.1 Medium 135/tcp

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

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

Quality of Detection: 80

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49664]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:127.0.0.1[49664]
      Annotation: KeyIso
Port: 49665/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49665]
Port: 49666/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49666]
      Annotation: Windows Event Log
Port: 49667/tcp
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
      UUID: 0f738e20-73c0-4ca8-aa6a-8dfef545fea8, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
      UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: IdSegSrv service
      UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
      UUID: 26268c86-e770-433e-86ef-5f3ba6731fba, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: Proxy Manager provider server endpoint
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: IP Transition Configuration endpoint
      UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
      UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: XactSrv service
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: Adh APIs
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: Impl friendly name
      UUID: e64b9aee-f372-4312-9a14-8f1502b5c8e3, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49667]
      Annotation: AppInfo
```

... continues on next page ...

... continued from previous page ...

```
Port: 49668/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49668]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49668]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49668]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49668]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:127.0.0.1[49668]
Port: 49673/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:127.0.0.1[49673]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

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

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

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

[return to 10.0.2.2]