Scan Report

July 25, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.58.0/24". The scan started at Tue Jul 23 21:15:53 2019 UTC and ended at Tue Jul 23 21:37:55 2019 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
192.168.58.3	22	62	7	0	0
192.168.58.1	0	0	1	0	0
Total: 2	22	62	8	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 92 results selected by the filtering described above. Before filtering there were 251 results.

2 Results per Host

2.1 192.168.58.3

Host scan start	Tue Jul 23 21:16:11 2019 UTC
Host scan end	Tue Jul 23 21:37:55 2019 UTC

Service (Port)	Threat Level
8022/tcp	High
80/tcp	High
3306/tcp	High
9200/tcp	High
22/tcp	High
445/tcp	High
8022/tcp	Medium
4848/tcp	Medium
8443/tcp	Medium
3306/tcp	Medium
21/tcp	Medium
8181/tcp	Medium
9200/tcp	Medium
135/tcp	Medium
22/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
3389/tcp	Medium
3306/tcp	Low
general/tcp	Low

2.1.1 High 8022/tcp

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

Product detection result

```
cpe:/a:zohocorp:manageengine_desktop_central:91084
Detected by ManageEngine Desktop Central MSP Version Detection (OID: 1.3.6.1.4.1
↪.25623.1.0.805717)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 91084
Fixed version:     100082
```

Solution

Solution type: VendorFix

Upgrade to build 100082 or later.

Affected Software/OS

ManageEngine Desktop Central before build 100082.

Vulnerability Detection Method

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

Details: `ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.106809

Version used: `$Revision: 12106 $`

Product Detection Result

Product: `cpe:/a:zohocorp:manageengine_desktop_central:91084`

Method: `ManageEngine Desktop Central MSP Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.805717)

References

```
CVE: CVE-2017-7213
Other:
```

... continues on next page ...

. . . continued from previous page . . .

URL:https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-control-privilege-violation.html

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central 9 FileUploadServlet connectionId Vulnerability

Product detection result

```
cpe:/a:zohocorp:manageengine_desktop_central:91084
Detected by ManageEngine Desktop Central MSP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.805717)
```

Summary

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

Vulnerability Detection Result

```
It was possible to upload the file ‘http://192.168.58.3:8022/jspf/OpenVAS-VT_CVE-2015-8249_test.jsp‘. Please delete this file.
```

Impact

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

Solution

Solution type: VendorFix

Update to ManageEngine Desktop Central 9, build 90142 or newer.

Affected Software/OS

ManageEngine Desktop Central 9 < build 90142.

Vulnerability Detection Method

Try to upload a jsp file.

Details: `ManageEngine Desktop Central 9 FileUploadServlet connectionId Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.140041

Version used: `$Revision: 13994 $`

Product Detection Result

Product: `cpe:/a:zohocorp:manageengine_desktop_central:91084`

Method: `ManageEngine Desktop Central MSP Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.805717)

References

CVE: CVE-2015-8249

High (CVSS: 7.5)
NVT: ManageEngine Desktop Central RCE Vulnerability

Product detection result

```
cpe:/a:zohocorp:manageengine_desktop_central:91084
Detected by ManageEngine Desktop Central MSP Version Detection (OID: 1.3.6.1.4.1
↪.25623.1.0.805717)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 91084
Fixed version:     100092
```

Solution

Solution type: VendorFix

Upgrade to build 100092 or later.

Affected Software/OS

ManageEngine Desktop Central before build 100092.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: `$Revision: 12106 $`

Product Detection Result

Product: `cpe:/a:zohocorp:manageengine_desktop_central:91084`
Method: `ManageEngine Desktop Central MSP Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.805717)

References

```
CVE: CVE-2017-11346
Other:
  URL:https://www.manageengine.com/products/desktop-central/remote-code-executio
↪n.html
```

High (CVSS: 7.5)
NVT: ZOHO ManageEngine Desktop Central Multiple Vulnerabilities-Apr18

Product detection result

```
cpe:/a:zohocorp:manageengine_desktop_central:91084
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by ManageEngine Desktop Central MSP Version Detection (OID: 1.3.6.1.4.1
↪.25623.1.0.805717)
```

Summary

This host is installed with ManageEngine Desktop Central and is prone to multiple vulnerabilities

Vulnerability Detection Result

```
Vulnerable url: http://192.168.58.3:8022/jsp/admin/DBQueryExecutor.jsp?actionFro
↪m=getResult&query=SELECT%20*%20from%20aaauser;
```

Impact

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

Solution

Solution type: VendorFix

Upgrade to ManageEngine Desktop Central build version 10.0.208 or later. Please see the references for more information.

Affected Software/OS

Zoho ManageEngine Desktop Central version 10.0.184 and prior.

Vulnerability Insight

Multiple flaws are due to,

- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts and
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

Vulnerability Detection Method

Send the crafted HTTP GET request and confirm SQL query execution from the response.

Details: `ZOHO ManageEngine Desktop Central Multiple Vulnerabilities-Apr18`

OID:1.3.6.1.4.1.25623.1.0.813213

Version used: `2019-05-03T08:55:39+0000`

Product Detection Result

Product: `cpe:/a:zohocorp:manageengine_desktop_central:91084`

Method: `ManageEngine Desktop Central MSP Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.805717)

References

```
CVE: CVE-2018-5337, CVE-2018-5338, CVE-2018-5339, CVE-2018-5341
Other:
  URL:https://www.manageengine.com
   URL:https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vu
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪lnerabilities-in-manageengine-desktop-central
```

[return to 192.168.58.3]

2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

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

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

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

Affected Software/OS
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: `MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2019-05-03T12:31:27+0000`

References

```
CVE: CVE-2015-1635
Other:
  URL:https://support.microsoft.com/kb/3042553
   URL:https://technet.microsoft.com/library/security/MS15-034
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
    URL:http://pastebin.com/ypURDPc4
```

[return to 192.168.58.3]

2.1.3 High 3306/tcp

High (CVSS: 10.0)
NVT: Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

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

Affected Software/OS

Oracle MySQL version 5.5.52 and earlier, 5.6.33 and earlier, 5.7.15 and earlier on Windows

Vulnerability Insight

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

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows`
OID:1.3.6.1.4.1.25623.1.0.809386
Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-5584, CVE-2016-6662, CVE-2016-7440
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.htm
↪l
```

High (CVSS: 10.0)
NVT: Oracle Mysql 'my.conf' Security Bypass Vulnerability (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.52
Installation
path / port:       3306/tcp
```

Impact

Successful exploitation will allow a local users to execute arbitrary code with root privileges by setting malloc_lib.

Solution

Solution type: VendorFix

Upgrade to Oracle MySQL Server 5.5.52, or 5.6.33, or 5.7.15, or later.

Affected Software/OS

Oracle MySQL Server before 5.5.52, 5.6.x before 5.6.33, and 5.7.x before 5.7.15 on windows.

Vulnerability Insight

The flaw exists due to datadir is writable by the mysqld server, and a user that can connect to MySQL can create 'my.cnf' in the datadir using 'SELECT ... OUTFILE'.

Vulnerability Detection Method

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

Details: `Oracle Mysql 'my.conf' Security Bypass Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.809330

Version used: `$Revision: 12983 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-6662
BID:92912
Other:
  URL:http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Executio
↪n-Privesc-CVE-2016-6662.txt
   URL:https://www.exploit-db.com/exploits/40360/
```

High (CVSS: 9.0)
NVT: MySQL / MariaDB weak password

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

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

Vulnerability Detection Result

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

Solution

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

Vulnerability Detection Method

Details: `MySQL / MariaDB weak password`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `$Revision: 12175 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

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

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

Impact

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

Solution

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

Affected Software/OS

Oracle MySQL Server version 5.5.40 and earlier, and 5.6.21 and earlier on Windows.

Vulnerability Insight

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

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805132
Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-0411, CVE-2014-6568, CVE-2015-0382, CVE-2015-0381, CVE-2015-0374
BID:72191, 72210, 72200, 72214, 72227
Other:
  URL:http://secunia.com/advisories/62525
```

. . . continues on next page . . .

. . . continued from previous page . . .

URL:http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html

High (CVSS: 7.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)

Product detection result
`cpe:/a:oracle:mysql:5.5.20`
`Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)`

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to 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
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL Server version 5.5.39 and earlier, and 5.6.20 and earlier on Windows.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804781
Version used: `$Revision: 12858 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2014-6559, CVE-2014-6555, CVE-2014-6507, CVE-2014-6500, CVE-2014-6496,
↪CVE-2014-6494, CVE-2014-6491, CVE-2014-6469, CVE-2014-6464
BID:70487, 70530, 70550, 70478, 70469, 70497, 70444, 70446, 70451
Other:
  URL:http://secunia.com/advisories/60599
   URL:http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
```

High (CVSS: 7.5)
NVT: Oracle Mysql Security Updates-02 (oct2018-4428296) Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from Reference links.

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 on Windows

Vulnerability Insight

Multiple flaws exists 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 Updates-02 (oct2018-4428296) Windows`
OID:1.3.6.1.4.1.25623.1.0.814258
Version used: `2019-07-05T09:12:25+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-3133, CVE-2018-3174, CVE-2018-3282, CVE-2016-9843
Other:
  URL:https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.ht
↪ml
```

High (CVSS: 7.5)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

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

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

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

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

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

. . . continues on next page . . .

... continued from previous page ...

Details: `Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.812650
Version used: `$Revision: 12047 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-2562
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.htm
↪l
```

High (CVSS: 7.2)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Feb16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact
Successful exploitation will allows 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 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 on windows

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

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-01 Feb16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.806876
Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-0609, CVE-2016-0608, CVE-2016-0606, CVE-2016-0600, CVE-2016-0598,
↪CVE-2016-0597, CVE-2016-0546, CVE-2016-0505
BID:81258, 81226, 81188, 81182, 81151, 81066, 81088
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
```

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

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL Server Server 5.5.44 and earlier, and 5.6.25 and earlier

Vulnerability Insight

Unspecified errors 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-06 Oct15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805769

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4879, CVE-2015-4819
BID:77140, 77196
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
```

High (CVSS: 7.2)

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

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.5.52
Installation
path / port:       3306/tcp
```

Impact

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

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Upgrade to Oracle MySQL Server 5.5.52 or later.

Affected Software/OS

Oracle MySQL Server 5.5.x to 5.5.51 on windows

Vulnerability Insight

Multiple errors exist. Please see the references for more information.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809300
Version used: `2019-05-03T13:51:56+0000`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

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

High (CVSS: 7.1)
NVT: Oracle MySQL Unspecified Vulnerability-01 July16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
Oracle MySQL Server 5.5.45 and earlier, 5.6.26 and earlier on windows

Vulnerability Insight
An unspecified error exist in the MySQL Server component via unknown vectors related to Option.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Unspecified Vulnerability-01 July16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.808591
Version used: `$Revision: 12983 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-3471
BID:91913
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.htm
↪l
```

[return to 192.168.58.3]

2.1.4 High 9200/tcp

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

Product detection result

```
cpe:/a:elasticsearch:elasticsearch:1.1.1
Detected by Elasticsearch and Logstash Detection (OID: 1.3.6.1.4.1.25623.1.0.105
↪031)
```

Summary
The script checks if the target host runs End of Life software. End of Life software doesn't receive any more updates and is highly prone to zero-day vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Solution

Solution type: VendorFix

Update Elasticsearch to a version that still receives technical support and updates.

Vulnerability Detection Method

Details: `Elasticsearch End of Life Detection`

OID:1.3.6.1.4.1.25623.1.0.113131

Version used: `$Revision: 12045 $`

Product Detection Result

Product: `cpe:/a:elasticsearch:elasticsearch:1.1.1`

Method: `Elasticsearch and Logstash Detection`

OID: 1.3.6.1.4.1.25623.1.0.105031)

References

```
Other:
  URL:https://www.elastic.co/support/eol
```

High (CVSS: 7.5)

NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)

Product detection result

```
cpe:/a:elasticsearch:elasticsearch:1.1.1
Detected by Elasticsearch and Logstash Detection (OID: 1.3.6.1.4.1.25623.1.0.105
↪031)
```

Summary

This host is running Elasticsearch and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     1.6.1
```

Impact

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

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade 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: `$Revision: 12363 $`

Product Detection Result
Product: `cpe:/a:elasticsearch:elasticsearch:1.1.1`
Method: `Elasticsearch and Logstash Detection`
OID: 1.3.6.1.4.1.25623.1.0.105031)

References
```
CVE: CVE-2015-5531, CVE-2015-5377
BID:75935
Other:
  URL:https://www.elastic.co/community/security/
   URL:http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded
```

[return to 192.168.58.3]

2.1.5 High 22/tcp

High (CVSS: 7.8)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)

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

Summary
This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.3 or later.

Affected Software/OS

OpenSSH versions before 7.3 on Windows

Vulnerability Insight

Multiple flaws exist due to,

- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.

- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method

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

Details: `OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)`

OID:1.3.6.1.4.1.25623.1.0.809121

Version used: `2019-05-21T12:48:06+0000`

Product Detection Result

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

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-6515, CVE-2016-6210
BID:92212
Other:
  URL:http://www.openssh.com/txt/release-7.3
   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
```

High (CVSS: 7.5)
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

This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.2 or later.

Affected Software/OS

OpenSSH versions before 7.2 on Windows

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: `OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.810768

Version used: `2019-05-21T12:48:06+0000`

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`

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:84427
Other:
  URL:http://openwall.com/lists/oss-security/2016/01/15/13
   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=ed4ce82dbfa8a3a3c8ea6f
↪a0db113c71e234416c
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741
```

High (CVSS: 7.5)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Windows)

Product detection result

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

Summary

This host is installed with openssh and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.4
Installation
path / port:       22/tcp
```

Impact

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

Solution

Solution type: VendorFix

Upgrade to OpenSSH version 7.4 or later.

Affected Software/OS

OpenSSH versions before 7.4 on Windows.

Vulnerability Insight

Multiple flaws exists 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.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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: `2019-05-21T12:48:06+0000`

Product Detection Result

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

Method: `OpenSSH Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10
↪708
BID:94968, 94972, 94977, 94975
Other:
  URL:https://www.openssh.com/txt/release-7.4
   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=28652bca29046f62c7045e
↪933e6b931de1d16737
```

[return to 192.168.58.3]

2.1.6 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary

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

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

Solution

Solution type: VendorFix

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight

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

Vulnerability Detection Method

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`

OID:1.3.6.1.4.1.25623.1.0.810676

Version used: `2019-05-03T10:54:50+0000`

References

```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

[return to 192.168.58.3]

2.1.7 Medium 8022/tcp

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

Summary

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

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.58.3:8022/configurations.do:j_password
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

[return to 192.168.58.3]

2.1.8 Medium 4848/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Untrusted Certificate Authorities

Summary

The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted Certi
↪ficate Authority:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ia,C=US
Certificate details:
subject ...: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Cal
↪ifornia,C=US
subject alternative names (SAN):
None
issued by .: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Cal
↪ifornia,C=US
serial ....: 04A9972F
valid from : 2013-05-15 05:33:38 UTC
valid until: 2023-05-13 05:33:38 UTC
fingerprint (SHA-1): 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256): AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD5B23381002A
↪885F556
```

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted certificate authority.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority.

Details: `SSL/TLS: Untrusted Certificate Authorities`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `$Revision: 11874 $`

Medium (CVSS: 5.0)

NVT: Oracle Glass Fish Server Directory Traversal Vulnerability

Summary

This host is installed with Glass fish server and is prone to directory traversal vulnerability.

Vulnerability Detection Result

```
Vulnerable url: https://192.168.58.3:4848/theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%
↪ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%
↪ae/%c0%ae%c0%ae/%c0%ae%c0%ae/windows/win.ini
```

Impact

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

Solution

Solution type: WillNotFix

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

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11702 $`

References

```
CVE: CVE-2017-1000028
Other:
  URL:https://www.exploit-db.com/exploits/39241
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

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

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

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

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`

. . . continues on next page . . .

. . . continued from previous page . . .

↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `$Revision: 12865 $`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 192.168.58.3]

2.1.9 Medium 8443/tcp

Medium (CVSS: 5.4)
NVT: SSL/TLS: Report 'Anonymous' Cipher Suites

Summary
This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_WITH_AES_128_CBC_SHA
```

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

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

Vulnerability Insight
Services supporting 'Anonymous' cipher suites could allow a client to negotiate a SSL/TLS connection to the host without any authentication of the remote endpoint.

Vulnerability Detection Method
Details: `SSL/TLS: Report 'Anonymous' Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.108147
Version used: `2019-05-10T14:24:23+0000`

References

```
CVE: CVE-2007-1858, CVE-2014-0351
BID:28482, 69754
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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

Vulnerability Detection Result
Server Temporary Key Size: 768 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (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: $Revision: 12865 $

References
Other:
URL:https://weakdh.org/
URL:https://weakdh.org/sysadmin.html

[return to 192.168.58.3]

2.1.10 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple denial-of-service vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation of these vulnerabilities will allow remote attackers to conduct a denial-of-service attack.

Solution

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

Affected Software/OS

Oracle MySQL version 5.5.58 and earlier, 5.6.38 and earlier, 5.7.20 and earlier on Windows

Vulnerability Insight

Multiple flaws exists 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: `$Revision: 12088 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-2668, CVE-2018-2665, CVE-2018-2622, CVE-2018-2640
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.htm
↪l
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 July16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 5.5.49 and earlier, 5.6.30 and earlier, 5.7.12 and earlier on windows

Vulnerability Insight

Multiple unspecified errors 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-01 July16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808588

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440
BID:91902, 91932, 91960, 91953
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.htm
↪l
```

Medium (CVSS: 6.8)
NVT: Oracle MySQL Security Updates (oct2016-2881722) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Mysql version 5.5.51 and earlier, 5.6.32 and earlier, 5.7.14 and earlier on Windows

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in '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 Security Updates (oct2016-2881722) 02 - Windows`

OID:1.3.6.1.4.1.25623.1.0.809372

Version used: `$Revision: 12983 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-3492, CVE-2016-5626, CVE-2016-5629, CVE-2016-5616, CVE-2016-5617,
↪CVE-2016-8283
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.htm
↪l
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 Oct14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to 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
Apply the patch from the referenced advisory.

Affected Software/OS

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 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

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 Oct14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804782
Version used: `$Revision: 11867 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-6551, CVE-2014-6530, CVE-2014-6505, CVE-2014-6495, CVE-2014-6484,
↪CVE-2014-6478, CVE-2014-6463, CVE-2014-4287, CVE-2014-4274
Other:
  URL:http://secunia.com/advisories/60599
   URL:http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
```

Medium (CVSS: 6.5)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

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

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

Affected Software/OS
Oracle MySQL version 5.5.37 and earlier and 5.6.17 and earlier on Windows.

Vulnerability Insight
Unspecified errors in the MySQL Server component via unknown vectors related to SRINFOSC and SRCHAR.

. . . 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-02 July14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804722
Version used: `$Revision: 11878 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-4258, CVE-2014-4260
BID:68564, 68573
Other:
  URL:http://secunia.com/advisories/59521
   URL:http://www.computerworld.com/s/article/9249690/Oracle_to_release_115_secu
↪rity_patches
   URL:http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
↪#AppendixMSQL
```

Medium (CVSS: 6.3)
NVT: Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to a security bypass vulnerability.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3305
BID:97023
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.htm
↪l
```

Medium (CVSS: 6.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11878 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-2430, CVE-2014-2431, CVE-2014-2436, CVE-2014-2440
BID:66858, 66890, 66896, 66850
Other:
  URL:http://secunia.com/advisories/57940
   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
```

Medium (CVSS: 6.0)

NVT: Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        3306/tcp
```

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL version 5.5.54 and earlier, 5.6.35 and earlier, 5.7.17 and earlier on Windows

Vulnerability Insight

Multiple flaws exists 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3309, CVE-2017-3308, CVE-2017-3329, CVE-2017-3456, CVE-2017-3453,
↪CVE-2017-3600, CVE-2017-3462, CVE-2017-3463, CVE-2017-3461, CVE-2017-3464
BID:97742, 97725, 97763, 97831, 97776, 97765, 97851, 97849, 97812, 97818
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.htm
↪l
```

Medium (CVSS: 5.7)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier on windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server : Optimizer, DDL, Server : Compiling, Server : Federated.

Vulnerability Detection Method

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

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805172

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-2571, CVE-2015-0505, CVE-2015-0501, CVE-2015-0499
BID:74095, 74112, 74070, 74115
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
```

Medium (CVSS: 5.0)

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

Product detection result

`cpe:/a:oracle:mysql:5.5.20`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-2573, CVE-2015-2568, CVE-2015-0441, CVE-2015-0433
BID:74078, 74073, 74103, 74089
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
```

Medium (CVSS: 5.0)

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

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to denial-of-service vulnerability.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

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

Vulnerability Insight

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

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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3302
BID:96162
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.htm
↪l
```

Medium (CVSS: 5.0)
NVT: Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to denial-of-service vulnerability.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.

Affected Software/OS

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

Vulnerability Insight

Multiple errors exists 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2017-3302
Other:
  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
```

Medium (CVSS: 5.0)
NVT: Oracle MySQL < 5.7.26, 8.0.x < 8.0.16 Security Update (2019-5072813) - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.26
Installation
path / port:       3306/tcp
```

Solution

Solution type: VendorFix

Update to version 5.7.26, 8.0.16 or later.

Affected Software/OS

MySQL 5.7.25 and prior, 8.0.15 and prior.

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 < 5.7.26, 8.0.x < 8.0.16 Security Update (2019-5072813) - Windows`
OID:1.3.6.1.4.1.25623.1.0.142399
Version used: `2019-05-13T11:27:46+0000`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2019-2581, CVE-2019-2628, CVE-2019-2566, CVE-2019-2592, CVE-2019-2632
Other:
  URL:https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.ht
↪ml#AppendixMSQL
```

Medium (CVSS: 4.9)

NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-06 April16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 5.5.47 and earlier, 5.6.28 and earlier, 5.7.10 and earlier on windows

Vulnerability Insight

Unspecified errors 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-06 April16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.807928

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-0649, CVE-2016-0650, CVE-2016-0644, CVE-2016-0646, CVE-2016-0640,
↪CVE-2016-0641
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.h
↪tml
```

Medium (CVSS: 4.9)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

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

Solution
Solution type: VendorFix
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 exists due to
- A flaw in the Client mysqldump component.
- A flaw in the Server: DDL component.
- A flaw in the C API component.
- A flaw in the Connector/C component.
- A flaw in the Server: Charsets component.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

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: $Revision: 11989 $

Product Detection Result
Product: cpe:/a:oracle:mysql:5.5.20
Method: MySQL/MariaDB Detection
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3651, CVE-2017-3653, CVE-2017-3652, CVE-2017-3635, CVE-2017-3648,
↪CVE-2017-3641
BID:99802, 99810, 99805, 99730, 99789, 99767
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.htm
↪l#AppendixMSQL
```

Medium (CVSS: 4.9)
NVT: Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to unspecified vulnerability.

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

Impact
Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

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

Affected Software/OS
Oracle MySQL versions 5.5.10 through 5.5.32 and 5.6.x through 5.6.12 on Windows

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11878 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2013-5807
BID:63105
Other:
  URL:http://secunia.com/advisories/55327
   URL:http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
```

Medium (CVSS: 4.9)

NVT: Oracle MySQL Security Updates-02 (jul2018-4258247) Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from Reference link.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL version 5.5.60 and earlier, 5.6.40 and earlier, 5.7.22 and earlier on Windows

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 Updates-02 (jul2018-4258247) Windows`
OID:1.3.6.1.4.1.25623.1.0.813706
Version used: `2019-05-17T10:45:27+0000`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-2767, CVE-2018-3066, CVE-2018-3058, CVE-2018-3070
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.htm
↪l
```

Medium (CVSS: 4.9)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

Vulnerability Insight
Multiple flaws exists 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: `$Revision: 12983 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3238, CVE-2017-3318, CVE-2017-3291, CVE-2017-3317, CVE-2017-3258,
↪CVE-2017-3312, CVE-2017-3313, CVE-2017-3244, CVE-2017-3265
BID:95571, 95560, 95491, 95527, 95565, 95588, 95501, 95585, 95520
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.htm
↪l
```

Medium (CVSS: 4.6)
NVT: Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to vulnerability.

Vulnerability Detection Result

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

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11989 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3636
BID:99736
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.htm
↪l#AppendixMSQL
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Unspecified Vulnerability-02 July16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:        3306/tcp
```

Impact

Successful exploitation will allows 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 5.5.48 and earlier, 5.6.29 and earlier, 5.7.11 and earlier on windows

Vulnerability Insight

An unspecified error exist in the MySQL Server component via unknown vectors related to Connection.

Vulnerability Detection Method

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

Details: `Oracle MySQL Unspecified Vulnerability-02 July16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808593

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-5444
BID:91987
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.htm
↪l
```

Medium (CVSS: 4.3)

NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 exists 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4737, CVE-2015-2620
BID:75802, 75837
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
```

Medium (CVSS: 4.3)

NVT: Oracle MySQL Backronym Vulnerability June16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running Oracle MySQL and is prone to the backronym vulnerability.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.7.3
```

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: `2019-07-05T09:12:25+0000`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-3152
Other:
  URL:http://www.ocert.org/advisories/ocert-2015-003.html
   URL:https://duo.com/blog/backronym-mysql-vulnerability
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Unspecified Vulnerability-03 July16 (Windows)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 5.5.48 and earlier, 5.6.29 and earlier, 5.7.10 and earlier on windows

Vulnerability Insight

An unspecified error exist in the MySQL Server component via unknown vectors related to Security Encryption.

Vulnerability Detection Method

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

Details: `Oracle MySQL Unspecified Vulnerability-03 July16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.808594

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-3452
BID:91999
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.htm
↪l
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL < 5.6.43, < 5.7.25, < 8.0.14 Security Update (2019-5072813) - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     5.6.43
Installation
path / port:       3306/tcp
```

Solution

Solution type: VendorFix

Update to version 5.6.43, 5.7.25, 8.0.14 or later.

Affected Software/OS

MySQL 5.6.42 and prior, 5.7.24 and prior, 8.0.13 and prior.

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 < 5.6.43, < 5.7.25, < 8.0.14 Security Update (2019-5072813) - Wind.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.142405

Version used: `2019-05-13T13:15:15+0000`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-3123
Other:
  URL:https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.ht
↪ml#AppendixMSQL
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 April16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows remote users 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 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier on windows

Vulnerability Insight

Unspecified errors 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-02 April16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807924
Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-0666, CVE-2016-0647, CVE-2016-0648, CVE-2016-0642, CVE-2016-0643,
↪CVE-2016-2047
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.h
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪tml
```

Medium (CVSS: 4.3)
NVT: Oracle MySQL < 5.6.44, < 5.7.26, < 8.0.16 Security Update (2019-5072813) - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

Oracle MySQL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
Fixed version:     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

MySQL 5.6.43 and prior, 5.7.25 and prior, 8.0.15 and prior.

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 < 5.6.44, < 5.7.26, < 8.0.16 Security Update (2019-5072813) - Wind.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.142403

Version used: `2019-05-13T13:15:15+0000`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2019-1559, CVE-2019-2683, CVE-2019-2627, CVE-2019-2614
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.ht
↪ml#AppendixMSQL
```

Medium (CVSS: 4.3)
NVT: Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the latest patch from vendor. Please see the references for more information.

Affected Software/OS

Oracle MySQL version 5.5.59 and earlier, 5.6.39 and earlier, 5.7.21 and earlier on Windows

Vulnerability Insight

Multiple flaws exists 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

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2019-05-17T10:45:27+0000`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-2761, CVE-2018-2771, CVE-2018-2781, CVE-2018-2773, CVE-2018-2817,
↪CVE-2018-2813, CVE-2018-2755, CVE-2018-2819, CVE-2018-2818
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.htm
↪l
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 Oct14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

Impact
Successful exploitation will allow attackers to 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
Apply the patch from the referenced advisory.

Affected Software/OS
MySQL Server version 5.5.38 and earlier on Windows.

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 Multiple Unspecified vulnerabilities-04 Oct14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804783
Version used: `$Revision: 11867 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-6520
BID:70510
Other:
  URL:http://secunia.com/advisories/60599
   URL:http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

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

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

Affected Software/OS
Oracle MySQL version 5.5.33 and earlier on Windows, Oracle MySQL version 5.6.13 and earlier on Windows

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804074
Version used: `$Revision: 11878 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2013-5891
BID:64891
Other:
  URL:http://secunia.com/advisories/56491
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 05 Jan14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

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

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

Affected Software/OS
Oracle MySQL version 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier on Windows.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11878 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-0386, CVE-2014-0393, CVE-2014-0402
BID:64904, 64877, 64908
Other:
  URL:http://secunia.com/advisories/56491
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Security Updates-04 (jul2018-4258247) Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to a denial-of-service vulnerability.

Vulnerability Detection Result

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

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

Solution
Solution type: VendorFix
Apply the patch from Reference link.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle MySQL version 5.5.60 and earlier on Windows

Vulnerability Insight
Multiple flaws exists 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 Updates-04 (jul2018-4258247) Windows`
OID:1.3.6.1.4.1.25623.1.0.813710
Version used: `2019-05-17T10:45:27+0000`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2018-3063
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.htm
↪l
```

Medium (CVSS: 4.0)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
Oracle MySQL version 5.5.57 and earlier, 5.6.37 and earlier, 5.7.19 and earlier on Windows.

Vulnerability Insight
Multiple flaws exists due to,
- An error in 'Client programs' component.
- An error in 'Server: DDL'.
- An error in 'Server: Replication'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows`
OID:1.3.6.1.4.1.25623.1.0.811991
Version used: `$Revision: 12983 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
CVE: CVE-2017-10379, CVE-2017-10384, CVE-2017-10268
BID:101415, 101406, 101390
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.htm
↪l
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Security Updates (oct2016-2881722) 05 - Windows

Product detection result
```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        3306/tcp
```

Impact

Successful exploitation of this vulnerability will allow 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 version 5.5.51 and earlier on Windows

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 Security Updates (oct2016-2881722) 05 - Windows`
OID:1.3.6.1.4.1.25623.1.0.809378
Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-5624
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.htm
↪l
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 5.5.20
```

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

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

Affected Software/OS
Oracle MySQL Server version 5.5.38 and earlier, and 5.6.19 and earlier on Windows.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities-04 Feb15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805135
Version used: `$Revision: 11872 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
CVE: CVE-2015-0391
BID:72205
Other:
  URL:http://secunia.com/advisories/62525
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Security Updates (oct2016-2881722) 03 - Windows

Product detection result
```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

. . . 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 a remote authenticated user to cause denial of service conditions.

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Mysql version 5.5.50 and earlier, 5.6.31 and earlier, and 5.7.13 and earlier on Windows

Vulnerability Insight

The flaw exists due to an unspecified error in Server: DML component.

Vulnerability Detection Method

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

Details: `Oracle MySQL Security Updates (oct2016-2881722) 03 - Windows`

OID:1.3.6.1.4.1.25623.1.0.809374

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-5612
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.htm
↪l
```

Medium (CVSS: 4.0)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 04 Jan14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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

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

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

Affected Software/OS
Oracle MySQL version 5.1.72 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: `$Revision: 11878 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
```
CVE: CVE-2014-0401, CVE-2014-0412, CVE-2014-0437, CVE-2013-5908
BID:64898, 64880, 64849, 64896
Other:
  URL:http://secunia.com/advisories/56491
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Unspecified Vulnerability-03 Feb16 (Windows)

Product detection result
```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 5.5.31 and earlier and 5.6.11 and earlier on windows

Vulnerability Insight

Unspecified errors 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 Unspecified Vulnerability-03 Feb16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.806878

Version used: `$Revision: 11989 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-0502
BID:81136
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
```

Medium (CVSS: 4.0)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.5.20
```

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server version 5.5.40 and earlier on Windows.

Vulnerability Insight

Unspecified errors in the MySQL Server component via unknown vectors related to Server:InnoDB:DDL:Foreign Key

Vulnerability Detection Method

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

Details: `Oracle MySQL Multiple Unspecified vulnerabilities-02 Feb15 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.805133

Version used: `$Revision: 11872 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-0432
BID:72217
Other:
  URL:http://secunia.com/advisories/62525
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
```

Medium (CVSS: 4.0)

NVT: MySQL Stored Procedure Unspecified Vulnerability (Windows)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

The host is running MySQL and is prone to multiple unspecified vulnerability.

Vulnerability Detection Result

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

Upgrade to MySQL version 5.5.31 or 5.6.11 or later.

Affected Software/OS

MySQL version 5.5.x before 5.5.31 and 5.6.x before 5.6.11. on Windows

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: `MySQL Stored Procedure Unspecified Vulnerability (Windows)`

OID:1.3.6.1.4.1.25623.1.0.809815

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2013-2376, CVE-2013-1511
BID:59227
Other:
  URL:http://secunia.com/advisories/53022
    URL:http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
    URL:http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪#AppendixMSQL
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-02 Jul15

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

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

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.43 and earlier, and 5.6.24 and earlier on Windows.

Vulnerability Insight

Unspecified errors exists 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2015-2648, CVE-2015-4752, CVE-2015-2643, CVE-2015-2582
BID:75822, 75849, 75830, 75751
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
```

Medium (CVSS: 4.0)
NVT: Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact

Successful exploitation of this vulnerability will allow remote attackers to 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-10378
BID:101375
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.htm
↪l
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Server Component 'Optimizer' Unspecified vulnerability Oct-2013 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to unspecified vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to disclose sensitive information, manipulate certain data, cause a DoS (Denial of Service) and bypass certain security restrictions.

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL versions 5.1.51 through 5.1.70, 5.5.10 through 5.5.32, and 5.6.x through 5.6.12 on Windows.

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: `$Revision: 11878 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2013-3839
BID:63109
Other:
  URL:http://secunia.com/advisories/55327
   URL:http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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 exists in the MySQL Server component via unknown vectors related to Server.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified Vulnerabilities-01 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805764
Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4913, CVE-2015-4830, CVE-2015-4826, CVE-2015-4815, CVE-2015-4807,
↪CVE-2015-4802, CVE-2015-4792, CVE-2015-4870, CVE-2015-4861, CVE-2015-4858, CVE
↪-2015-4836
BID:77153, 77228, 77237, 77222, 77205, 77165, 77171, 77208, 77137, 77145, 77190
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-08 Oct15 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows 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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4816
BID:77134
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
```

Medium (CVSS: 4.0)
NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 01 May14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

Solution

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

Affected Software/OS

Oracle MySQL version 5.5.35 and earlier and 5.6.15 and earlier on Windows.

. . . 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: `$Revision: 11878 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-0384, CVE-2014-2419, CVE-2014-2438
BID:66835, 66880, 66846
Other:
  URL:http://secunia.com/advisories/57940
   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
```

[return to 192.168.58.3]

2.1.11 Medium 21/tcp

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

Summary

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

Vulnerability Detection Result

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

Impact

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 13611 $`

[return to 192.168.58.3]

2.1.12 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Untrusted Certificate Authorities

Summary
The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted Certi
↪ficate Authority:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
subject ...: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Cal
↪ifornia,C=US
subject alternative names (SAN):
None
issued by .: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Cal
↪ifornia,C=US
serial ....: 04A9972F
valid from : 2013-05-15 05:33:38 UTC
valid until: 2023-05-13 05:33:38 UTC
fingerprint (SHA-1): 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256): AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD5B23381002A
↪885F556
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority.

Details: `SSL/TLS: Untrusted Certificate Authorities`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `$Revision: 11874 $`

Medium (CVSS: 4.0)

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

Summary

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

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

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

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: `$Revision: 12865 $`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 192.168.58.3]

2.1.13 Medium 9200/tcp

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

Product detection result

```
cpe:/a:elasticsearch:elasticsearch:1.1.1
Detected by Elasticsearch and Logstash Detection (OID: 1.3.6.1.4.1.25623.1.0.105
↪031)
```

Summary

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

Vulnerability Detection Result

```
Vulnerable url: http://192.168.58.3:9200/_search?source=%7B%22size%22%3A1%2C%22q
↪uery%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%
↪7D%7D%2C%22script_fields%22%3A%7B%22OpenVAS%22%3A%7B%22script%22%3A%22import%2
↪0java.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2F
↪windows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5CZ%5C%22).next()%3B%22
↪%7D%7D%7D&callback=?
```

Impact

An attacker can exploit this issue to execute arbitrary code

Solution

Solution type: VendorFix

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

Affected Software/OS

Elasticsearch < 1.2

Vulnerability Insight

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

Vulnerability Detection Method

Send a special crafted HTTP GET request and check the response
Details: `Elastisearch Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105032
Version used: `$Revision: 10833 $`

Product Detection Result

Product: `cpe:/a:elasticsearch:elasticsearch:1.1.1`
Method: `Elasticsearch and Logstash Detection`
OID: 1.3.6.1.4.1.25623.1.0.105031)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2014-3120
Other:
  URL:http://bouk.co/blog/elasticsearch-rce/
```

Medium (CVSS: 4.3)
NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)

Product detection result

```
cpe:/a:elasticsearch:elasticsearch:1.1.1
Detected by Elasticsearch and Logstash Detection (OID: 1.3.6.1.4.1.25623.1.0.105
↪031)
```

Summary

This host is running Elasticsearch and is prone to Cross-site Scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.1
Fixed version:     1.4.0.Beta1
```

Impact

Successful exploitation will allows remote attackers to inject arbitrary web script or HTML.

Solution

Solution type: VendorFix

Upgrade 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: `$Revision: 12431 $`

Product Detection Result

Product: `cpe:/a:elasticsearch:elasticsearch:1.1.1`
Method: `Elasticsearch and Logstash Detection`
OID: 1.3.6.1.4.1.25623.1.0.105031)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2014-6439
BID:70233
Other:
  URL:https://www.elastic.co/community/security/
   URL:http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded
```

[return to 192.168.58.3]

2.1.14 Medium 135/tcp

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

Summary

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

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49154]
     Annotation: Impl friendly name
Port: 49156/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49156]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49204/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.58.3[49204]
Port: 49254/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49254]
     Annotation: IPSec Policy agent endpoint
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.58.3[49254]
     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: `$Revision: 6319 $`

[return to 192.168.58.3]

2.1.15 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (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

This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.8
Installation
path / port:       22/tcp
```

Impact

Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution

Solution type: VendorFix

Update to version 7.8 or later.

Affected Software/OS

OpenSSH version 7.7 and prior on Windows.

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 User Enumeration Vulnerability-Aug18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2019-05-21T12:48:06+0000`

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
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Medium (CVSS: 5.0)
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

This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     None
Installation
path / port:       22/tcp
```

Impact

Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution

Solution type: NoneAvailable

No known solution is available as of 21th May, 2019. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

OpenSSH version 5.9 to 7.8 on Windows.

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: `2019-05-21T12:48:06+0000`

Product Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
CVE: CVE-2018-15919
Other:
  URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

Medium (CVSS: 5.0)
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
This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.6
Installation
path / port:       22/tcp
```

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

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.6 or later.

Affected Software/OS
OpenSSH versions before 7.6 on Windows

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812050

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2019-05-21T12:48:06+0000`

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
BID:101552
Other:
  URL:https://www.openssh.com/txt/release-7.6
   URL:https://github.com/openbsd/src/commit/a6981567e8e
```

[return to 192.168.58.3]

2.1.16 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with ’Opportunistic TLS’ and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

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

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium

. . . continues on next page . . .

. . . continued from previous page . . .

- 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: `$Revision: 11135 $`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:               CN=metasploitable3-win2k8
Signature Algorithm:   sha1WithRSAEncryption
```

Solution

Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 11524 $`

References

```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

[return to 192.168.58.3]

2.1.17 Low 3306/tcp

Low (CVSS: 3.5)
NVT: Oracle Mysql Security Updates (jan2017-2881727) 04 - Windows

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact
Successful exploitation of this vulnerability will allow remote to have some unspecified impact on availability.

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2017-3243
BID:95538
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.htm
↪l
```

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-04 Jul15

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to unspecified vulnerability.

Vulnerability Detection Result

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

Impact

Successful exploitation will allows an authenticated remote attacker to cause denial of service attack.

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12983 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4757
BID:75759
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
```

Low (CVSS: 3.5)
NVT: Oracle MySQL Unspecified Vulnerability-01 April16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

Impact
Successful exploitation will allows local users to affect availability.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle MySQL Server 5.5.46 and earlier on windows

Vulnerability Insight

Unspecified error exist 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 Unspecified Vulnerability-01 April16 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.807922

Version used: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2016-0651
Other:
  URL:http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.h
↪tml
```

Low (CVSS: 3.5)

NVT: Oracle MySQL Multiple Unspecified Vulnerabilities-07 Oct15 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allows 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: `$Revision: 12983 $`

Product Detection Result

Product: `cpe:/a:oracle:mysql:5.5.20`

Method: `MySQL/MariaDB Detection`

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2015-4864
BID:77187
Other:
  URL:http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
```

Low (CVSS: 2.8)

NVT: Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

This host is running Oracle MySQL and is prone to multiple unspecified vulnerabilities.

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 5.5.34 and earlier, and 5.6.14 and earlier on Windows.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle MySQL Multiple Unspecified vulnerabilities - 06 Jan14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804077
Version used: `$Revision: 11878 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2014-0420
BID:64888
Other:
  URL:http://secunia.com/advisories/56491
   URL:http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
```

Low (CVSS: 1.5)
NVT: Oracle MySQL Unspecified Vulnerability-01 Nov16 (Windows)

Product detection result

```
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary
This host is running Oracle MySQL and is prone to an unspecified vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

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

Impact
Successful exploitation will allow local users to affect availability.

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

Affected Software/OS
Oracle MySQL Server 5.5.30 and earlier and 5.6.9 and earlier on windows.

Vulnerability Insight
An unspecified error exist 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 Unspecified Vulnerability-01 Nov16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.809813
Version used: `$Revision: 12983 $`

Product Detection Result
Product: `cpe:/a:oracle:mysql:5.5.20`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

```
CVE: CVE-2013-1502
BID:59239
Other:
  URL:http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.
↪html
```

[return to 192.168.58.3]

2.1.18 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 103860266
Packet 2: 103860376
```

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/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 192.168.58.3]

2.2 192.168.58.1

Host scan start	Tue Jul 23 21:16:11 2019 UTC
Host scan end	Tue Jul 23 21:22:23 2019 UTC

Service (Port)	Threat Level
general/tcp	Low

2.2.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2071026505
Packet 2: 2071027580
```

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/IPv4 implementations that implement RFC1323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

. . . continues on next page . . .

. . . continued from previous page . . .

URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 192.168.58.1]