Vulnerability Discovery Results

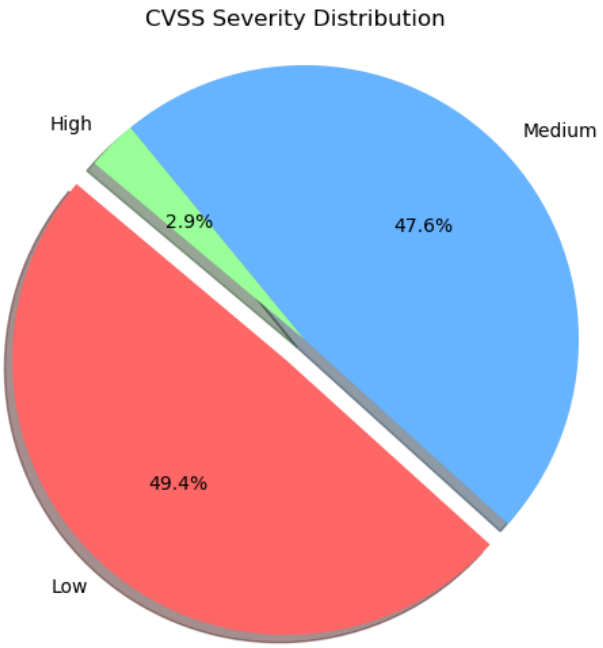
Friday 5th July, 2024

10:24

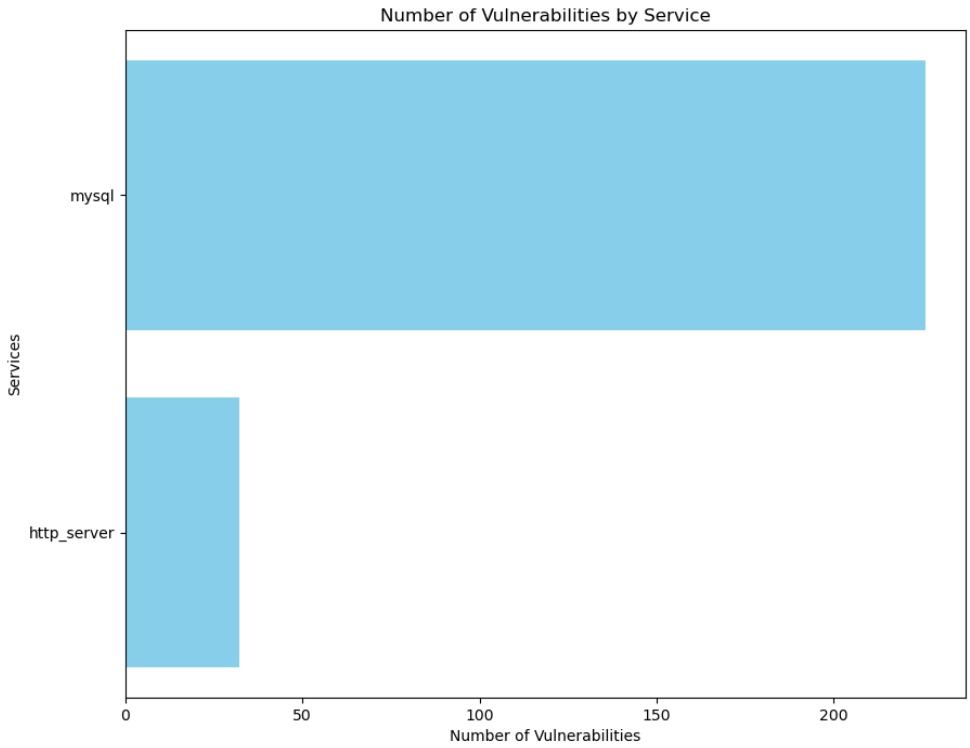
(UTC+2, PARIS)

Company Name	First Name	Last Name
Debian	Jenine	Ruddle

Name	OS Name	OS SP
victim2	Linux	4.0.x



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2016-9841

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

CVSS: 7.5

1.2 CVE-2016-9843

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.

CVSS: 7.5

1.3 CVE-2018-2562

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 7.5

1.4 CVE-2020-14760

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 7.5

1.5 CVE-2013-2395

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-1567.

CVSS: 6.8

1.6 CVE-2013-5860

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.

CVSS: 6.8

1.7 CVE-2013-5882

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedures.

CVSS: 6.8

1.8 CVE-2016-0504

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0503.

CVSS: 6.8

1.9 CVE-2016-3518

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.

CVSS: 6.8

1.10 CVE-2016-9840

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

CVSS: 6.8

1.11 CVE-2016-9842

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.

CVSS: 6.8

1.12 CVE-2018-2622

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.13 CVE-2018-2640

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.14 CVE-2018-2665

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.15 CVE-2018-2668

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.16 CVE-2020-14814

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.17 CVE-2020-14830

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.18 CVE-2020-14837

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.19 CVE-2020-14839

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.20 CVE-2020-14845

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.21 CVE-2020-14846

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.22 CVE-2020-14852

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.23 CVE-2014-2444

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to InnoDB.

CVSS: 6.5

1.24 CVE-2014-2484

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SRFTS.

CVSS: 6.5

1.25 CVE-2015-2617

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Partition.

CVSS: 6.5

1.26 CVE-2017-3305

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.5.55 and earlier and 5.6.35 and earlier. Difficult to exploit vulnerability allows low privileged 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. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue allows man-in-the-middle attackers to hijack the authentication of users by leveraging incorrect ordering of security parameter verification in a client, aka, “The Riddle”.

CVSS: 6.3

1.27 CVE-2017-3600

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:

CVSS: 6.0

1.28 CVE-2013-3798

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect integrity and availability via unknown vectors related to MemCached.

CVSS: 5.8

1.29 CVE-2017-3454

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 5.5

1.30 CVE-2017-3455

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).

CVSS: 5.5

1.31 CVE-2019-2731

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).

CVSS: 5.5

1.32 CVE-2013-1570

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote attackers to affect availability via unknown vectors related to MemCached.

CVSS: 5.0

1.33 CVE-2017-3329

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Thread Pooling). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/

CVSS: 5.0

1.34 CVE-2020-1967

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

CVSS: 5.0

1.35 CVE-2016-3588

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect integrity and availability via vectors related to Server: InnoDB.

CVSS: 4.9

1.36 CVE-2017-3265

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).

CVSS: 4.9

1.37 CVE-2017-3652

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier,

5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).

CVSS: 4.9

1.38 CVE-2018-3066

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).

CVSS: 4.9

1.39 CVE-2018-3081

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 4.9

1.40 CVE-2021-2356

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 4.9

1.41 CVE-2017-3636

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).

CVSS: 4.6

1.42 CVE-2014-0433

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote attackers to affect availability via unknown vectors related to Thread Pooling.

CVSS: 4.3

1.43 CVE-2016-0594

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.21 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.3

1.44 CVE-2015-3152

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the –ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a “BACKRONYM” attack.

CVSS: 4.3

1.45 CVE-2017-3467

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.7.17 and earlier. 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/

CVSS: 4.3

1.46 CVE-2017-3650

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions that are affected are 5.7.18 and earlier. 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/

CVSS: 4.3

1.47 CVE-2018-2761

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.3

1.48 CVE-2018-0735

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).

CVSS: 4.3

1.49 CVE-2020-1971

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL

embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

CVSS: 4.3

1.50 CVE-2013-3795

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.

CVSS: 4.0

1.51 CVE-2013-3796

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.

CVSS: 4.0

1.52 CVE-2013-3806

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3811.

CVSS: 4.0

1.53 CVE-2013-3807

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Server Privileges.

CVSS: 4.0

1.54 CVE-2013-5767

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.55 CVE-2013-5786

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5793.

CVSS: 4.0

1.56 CVE-2013-5894

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 4.0

1.57 CVE-2013-5881

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2014-0431.

CVSS: 4.0

1.58 CVE-2014-2434

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.59 CVE-2014-2435

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.16 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 4.0

1.60 CVE-2014-2442

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to MyISAM.

CVSS: 4.0

1.61 CVE-2014-2450

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.62 CVE-2014-4233

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRREP.

CVSS: 4.0

1.63 CVE-2014-4238

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SROPTZR.

CVSS: 4.0

1.64 CVE-2015-0409

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.65 CVE-2015-0405

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA.

CVSS: 4.0

1.66 CVE-2015-0423

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.67 CVE-2015-0438

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.68 CVE-2015-0439

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-4756.

CVSS: 4.0

1.69 CVE-2015-0500

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors.

CVSS: 4.0

1.70 CVE-2015-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.71 CVE-2015-0508

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-0506.

CVSS: 4.0

1.72 CVE-2015-4756

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-0439.

CVSS: 4.0

1.73 CVE-2015-4772

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.74 CVE-2015-4730

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.20 and earlier allows remote authenticated users to affect availability via unknown vectors related to Types.

CVSS: 4.0

1.75 CVE-2015-4800

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.

CVSS: 4.0

1.76 CVE-2015-4833

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.77 CVE-2015-4862

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.78 CVE-2015-4904

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to libmysqld.

CVSS: 4.0

1.79 CVE-2015-4905

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML.

CVSS: 4.0

1.80 CVE-2016-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0504.

CVSS: 4.0

1.81 CVE-2016-0595

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.82 CVE-2016-0611

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.83 CVE-2016-3424

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.

CVSS: 4.0

1.84 CVE-2016-3440

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.

CVSS: 4.0

1.85 CVE-2016-5436

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.

CVSS: 4.0

1.86 CVE-2016-5437

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Log.

CVSS: 4.0

1.87 CVE-2016-5441

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.
CVSS: 4.0

1.88 CVE-2016-5442

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption.
CVSS: 4.0

1.89 CVE-2016-5628

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: DML.
CVSS: 4.0

1.90 CVE-2016-5631

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Memcached.
CVSS: 4.0

1.91 CVE-2016-5632

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.
CVSS: 4.0

1.92 CVE-2016-5633

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*
Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-8290.
CVSS: 4.0

1.93 CVE-2016-5634

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to RBR.

CVSS: 4.0

1.94 CVE-2016-5635

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Audit.

CVSS: 4.0

1.95 CVE-2017-3238

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVSS: 4.0

1.96 CVE-2017-3244

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVSS: 4.0

1.97 CVE-2017-3251

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.9 (Availability impacts).

CVSS: 4.0

1.98 CVE-2017-3256

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVSS: 4.0

1.99 CVE-2017-3258

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVSS: 4.0

1.100 CVE-2017-3308

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily “exploitable” vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVSS: 4.0

1.101 CVE-2017-3309

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily “exploitable” vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).

CVSS: 4.0

1.102 CVE-2017-3452

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.35 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.103 CVE-2017-3453

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS: 4.0

1.104 CVE-2017-3456

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.105 CVE-2017-3457

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.106 CVE-2017-3458

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.107 CVE-2017-3459

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.108 CVE-2017-3460

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.109 CVE-2017-3461

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.110 CVE-2017-3462

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.111 CVE-2017-3463

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.112 CVE-2017-3464

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.113 CVE-2017-3465

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.114 CVE-2017-3638

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.115 CVE-2017-3639

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.116 CVE-2017-3640

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.117 CVE-2017-3641

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.118 CVE-2017-3642

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.119 CVE-2017-3643

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.120 CVE-2017-3644

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.121 CVE-2017-3645

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.122 CVE-2017-3646

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.123 CVE-2017-3648

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.124 CVE-2017-3651

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.125 CVE-2017-10165

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.126 CVE-2017-10167

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.127 CVE-2017-10284

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Stored Procedure). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.128 CVE-2017-10296

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.129 CVE-2017-10311

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.130 CVE-2017-10313

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.131 CVE-2017-10378

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.132 CVE-2017-10379

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged 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. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).

CVSS: 4.0

1.133 CVE-2017-10384

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.134 CVE-2018-2781

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.135 CVE-2018-2813

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.136 CVE-2018-2817

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.137 CVE-2018-2818

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVSS: 4.0

1.138 CVE-2018-2819

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.139 CVE-2018-3058

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.140 CVE-2018-3061

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.141 CVE-2018-3063

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.142 CVE-2018-3070

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.143 CVE-2018-3071

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.144 CVE-2018-3133

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS: 4.0

1.145 CVE-2018-3282

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.146 CVE-2019-2755

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.147 CVE-2019-2757

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.148 CVE-2022-21417

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.149 CVE-2018-2755

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).

CVSS: 3.7

1.150 CVE-2014-4240

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows local users to affect confidentiality and integrity via vectors related to SRREP.

CVSS: 3.6

1.151 CVE-2013-1566

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 3.5

1.152 CVE-2013-1567

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-2395.

CVSS: 3.5

1.153 CVE-2013-2381

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server Privileges.

CVSS: 3.5

1.154 CVE-2013-3810

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA Transactions.

CVSS: 3.5

1.155 CVE-2013-3811

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3806.

CVSS: 3.5

1.156 CVE-2013-5793

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5786.

CVSS: 3.5

1.157 CVE-2014-0427

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via vectors related to FTS.

CVSS: 3.5

1.158 CVE-2014-0431

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5881.

CVSS: 3.5

1.159 CVE-2014-2451

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Privileges.

CVSS: 3.5

1.160 CVE-2015-0385

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Pluggable Auth.

CVSS: 3.5

1.161 CVE-2015-0506

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2015-0508.

CVSS: 3.5

1.162 CVE-2015-0507

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.
CVSS: 3.5

1.163 CVE-2015-2567

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.
CVSS: 3.5

1.164 CVE-2015-2639

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Firewall.
CVSS: 3.5

1.165 CVE-2015-2641

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.
CVSS: 3.5

1.166 CVE-2015-4761

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.
CVSS: 3.5

1.167 CVE-2015-4769

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4767.
CVSS: 3.5

1.168 CVE-2015-4771

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to RBR.

CVSS: 3.5

1.169 CVE-2015-4791

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.

CVSS: 3.5

1.170 CVE-2015-4890

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Replication.

CVSS: 3.5

1.171 CVE-2016-0610

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and MariaDB before 10.0.22 and 10.1.x before 10.1.9 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 3.5

1.172 CVE-2016-0652

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to DML.

CVSS: 3.5

1.173 CVE-2016-0653

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to FTS.

CVSS: 3.5

1.174 CVE-2016-0654

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0656.

CVSS: 3.5

1.175 CVE-2016-0656

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0654.

CVSS: 3.5

1.176 CVE-2016-0657

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect confidentiality via vectors related to JSON.

CVSS: 3.5

1.177 CVE-2016-0658

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Optimizer.

CVSS: 3.5

1.178 CVE-2016-0659

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Optimizer.

CVSS: 3.5

1.179 CVE-2016-0662

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Partition.

CVSS: 3.5

1.180 CVE-2016-0663

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Performance Schema.

CVSS: 3.5

1.181 CVE-2016-8286

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote authenticated users to affect confidentiality via vectors related to Server: Security: Privileges.

CVSS: 3.5

1.182 CVE-2016-8287

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.

CVSS: 3.5

1.183 CVE-2016-8290

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-5633.

CVSS: 3.5

1.184 CVE-2017-3243

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).

CVSS: 3.5

1.185 CVE-2017-3291

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts).

CVSS: 3.5

1.186 CVE-2017-3312

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts).

CVSS: 3.5

1.187 CVE-2017-3319

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 3.1 (Confidentiality impacts).

CVSS: 3.5

1.188 CVE-2017-3320

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 2.4 (Confidentiality impacts).

CVSS: 3.5

1.189 CVE-2017-3468

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 3.5

1.190 CVE-2017-3529

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: UDF). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.191 CVE-2017-3635

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/C). Supported versions that are affected are 6.1.10 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. Note: The documentation has also been updated for the correct way to use mysql_stmt_close(). Please see: https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-execute.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-fetch.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-close.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-error.html, https://dev.mysql.com/man/5.7/en/mysql-stmt-errno.html, and https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-sqlstate.html. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.192 CVE-2017-3637

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.193 CVE-2017-3653

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server.

Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 3.5

1.194 CVE-2018-2771

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.195 CVE-2018-2767

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).

CVSS: 3.5

1.196 CVE-2019-2741

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.197 CVE-2014-4214

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRSP.

CVSS: 3.3

1.198 CVE-2016-8289

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows local users to affect integrity and availability via vectors related to Server: InnoDB.

CVSS: 3.3

1.199 CVE-2014-0430

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Performance Schema.

CVSS: 2.8

1.200 CVE-2015-0511

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : SP.

CVSS: 2.8

1.201 CVE-2015-2566

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 2.8

1.202 CVE-2016-0607

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to replication.

CVSS: 2.8

1.203 CVE-2016-0667

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Locking.

CVSS: 2.8

1.204 CVE-2019-7317

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
CVSS: 2.6

1.205 CVE-2013-5770

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Locking.
CVSS: 2.1

1.206 CVE-2015-2661

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows local users to affect availability via unknown vectors related to Client.
CVSS: 2.1

1.207 CVE-2015-4910

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.
CVSS: 2.1

1.208 CVE-2020-15358

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.
CVSS: 2.1

1.209 CVE-2021-22570

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*
Summary: Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.
CVSS: 2.1

1.210 CVE-2022-21444

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 2.1

1.211 CVE-2015-4766

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows local users to affect availability via unknown vectors related to Server : Security : Firewall.

CVSS: 1.9

1.212 CVE-2018-2773

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 1.9

1.213 CVE-2018-3174

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H).

CVSS: 1.9

1.214 CVE-2015-0498

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Replication.

CVSS: 1.7

1.215 CVE-2015-4767

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4769.

CVSS: 1.7

1.216 CVE-2017-3313

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes 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. CVSS v3.0 Base Score 4.7 (Confidentiality impacts).

CVSS: 1.5

1.217 CVE-2017-3317

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).

CVSS: 1.5

1.218 CVE-2017-10268

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes 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. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).

CVSS: 1.5

1.219 CVE-2016-5443

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection.

CVSS: 1.2

1.220 CVE-2017-3318

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).

CVSS: 1.0

1.221 CVE-2023-21977

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.222 CVE-2023-21980

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).

CVSS: N/A

1.223 CVE-2023-22007

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.224 CVE-2023-22015

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.225 CVE-2023-22026

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.226 CVE-2023-22028

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.53:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.227 CVE-2021-26691

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

CVSS: 7.5

1.228 CVE-2021-39275

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 7.5

1.229 CVE-2021-44790

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

CVSS: 7.5

1.230 CVE-2022-22720

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CVSS: 7.5

1.231 CVE-2022-23943

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

CVSS: 7.5

1.232 CVE-2022-31813

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

CVSS: 7.5

1.233 CVE-2020-35452

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

CVSS: 6.8

1.234 CVE-2021-40438

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 6.8

1.235 CVE-2021-44224

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

CVSS: 6.4

1.236 CVE-2022-28615

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

CVSS: 6.4

1.237 CVE-2022-22721

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.8

1.238 CVE-2019-17567

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

CVSS: 5.0

1.239 CVE-2020-13950

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

CVSS: 5.0

1.240 CVE-2021-26690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

CVSS: 5.0

1.241 CVE-2021-30641

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

CVSS: 5.0

1.242 CVE-2021-33193

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

CVSS: 5.0

1.243 CVE-2021-34798

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 5.0

1.244 CVE-2021-36160

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

CVSS: 5.0

1.245 CVE-2022-22719

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.0

1.246 CVE-2022-26377

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

CVSS: 5.0

1.247 CVE-2022-28330

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

CVSS: 5.0

1.248 CVE-2022-28614

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

CVSS: 5.0

1.249 CVE-2022-29404

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

CVSS: 5.0

1.250 CVE-2022-30556

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

CVSS: 5.0

1.251 CVE-2020-13938

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

CVSS: 2.1

1.252 CVE-2006-20001

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

This issue affects Apache HTTP Server 2.4.54 and earlier.

CVSS: N/A

1.253 CVE-2022-36760

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

CVSS: N/A

1.254 CVE-2022-37436

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVSS: N/A

1.255 CVE-2023-25690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::*

Summary: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:

RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

CVSS: N/A

1.256 CVE-2023-27522

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::::*

Summary: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

CVSS: N/A

1.257 CVE-2023-31122

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::::*

Summary: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS: N/A

1.258 CVE-2023-45802

!–> CVE for cpe:2.3:a:apache:http_server:2.4.46:::::::*

Summary: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.

Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS: N/A