Pentests Results

Company Name	First Name	Last Name
JD	John	Doe

Name	OS Name	OS SP
plin12	Linux	2.4.x

Details

1.1 CVE-2021-3618

!–> CVE for cpe:2.3:a:vsftpd_project:vsftpd:3.0.3:::::::

Summary: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

CVSS: 5.8

1.2 CVE-2021-30047

!–> CVE for cpe:2.3:a:vsftpd_project:vsftpd:3.0.3:::::::

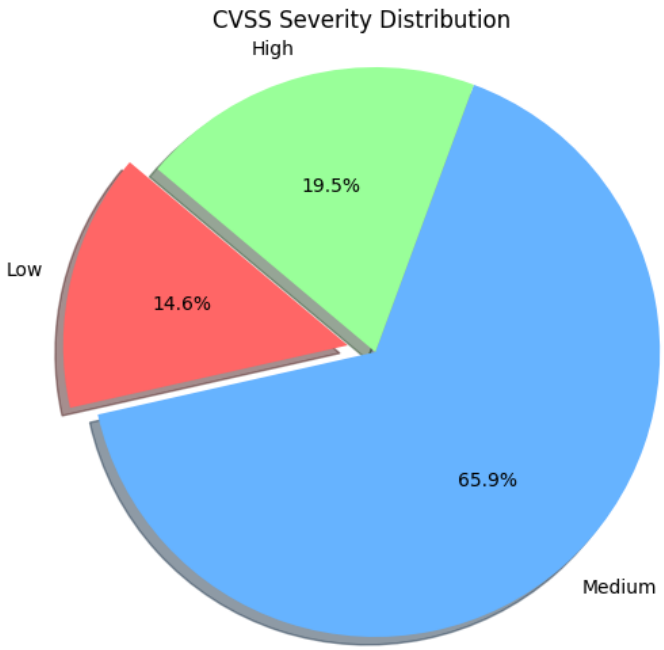
Summary: VSFTPD 3.0.3 allows attackers to cause a denial of service due to limited number of connections allowed.

CVSS: N/A

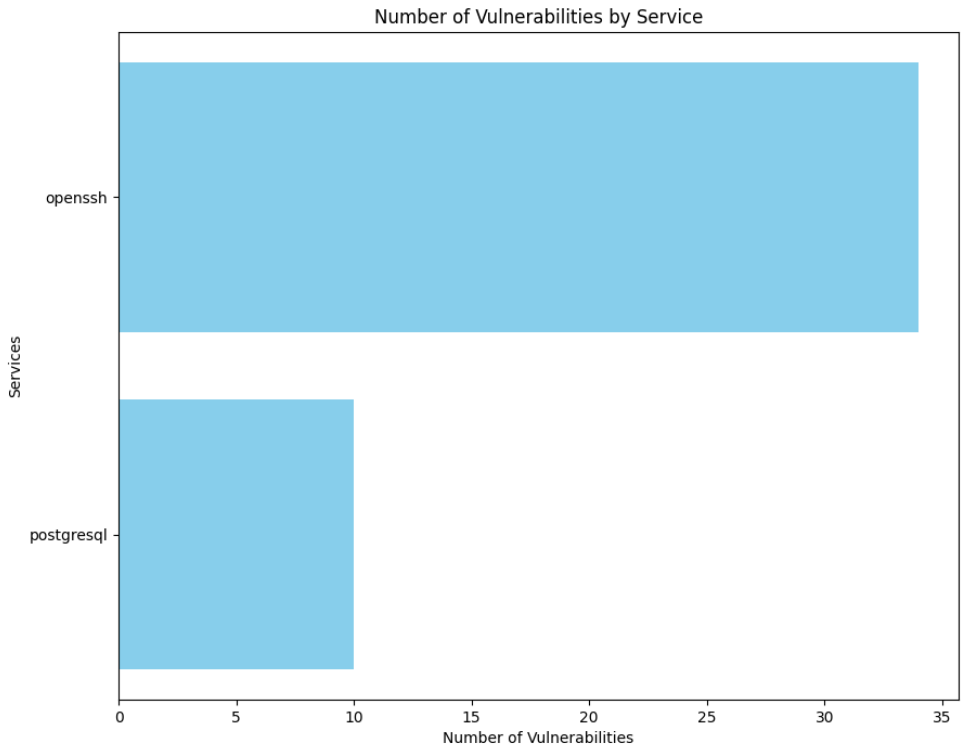
1.3 CVE-2020-14878

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVSS: 7.7

1.4 CVE-2020-5398

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: In Spring Framework, versions 5.2.x prior to 5.2.3, versions 5.1.x prior to 5.1.13, and versions 5.0.x prior to 5.0.16, an application is vulnerable to a reflected file download (RFD) attack when it sets a "Content-Disposition" header in the response where the filename attribute is derived from user supplied input.
CVSS: 7.6

1.5 CVE-2016-9843

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
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

1.6 CVE-2019-14540

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariConfig.
CVSS: 7.5

1.7 CVE-2020-11656

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.
CVSS: 7.5

1.8 CVE-2016-9841

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
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

1.9 CVE-2021-2011

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated 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. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

CVSS: 7.1

1.10 CVE-2021-2048

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 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 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 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 7.0

1.11 CVE-2020-14869

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 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

1.12 CVE-2016-9840

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.13 CVE-2021-2354

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 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

1.14 CVE-2020-14672

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 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

1.15 CVE-2020-14852

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.16 CVE-2020-14848

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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-2020-14866

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.18 CVE-2021-2016

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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-2020-14861

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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-2021-2020

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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 3.1 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

1.21 CVE-2021-2076

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.22 CVE-2021-2060

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 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 3.1 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-2019-2830

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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: 6.8

1.24 CVE-2021-35537

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 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

1.25 CVE-2021-2030

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.26 CVE-2020-14814

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.27 CVE-2020-14829

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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

1.28 CVE-2020-14846

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.29 CVE-2021-2072

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 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 3.1 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

1.30 CVE-2022-21253

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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

1.31 CVE-2021-35637

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 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

1.32 CVE-2016-9842

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.33 CVE-2021-2122

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 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 3.1 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

1.34 CVE-2020-14812

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and

prior and 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

1.35 CVE-2021-2339

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 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

1.36 CVE-2020-14830

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.37 CVE-2020-14836

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.38 CVE-2022-21256

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27

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

1.39 CVE-2020-14873

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 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 3.1 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: 6.8

1.40 CVE-2021-2002

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 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 3.1 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

1.41 CVE-2021-2065

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.42 CVE-2021-2036

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.43 CVE-2021-2031

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.44 CVE-2020-14821

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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

1.45 CVE-2020-14839

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.46 CVE-2019-2834

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 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

1.47 CVE-2020-14844

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). 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

1.48 CVE-2021-35638

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.49 CVE-2021-2028

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). 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

1.50 CVE-2020-14870

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). 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

1.51 CVE-2021-2001

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.30 and prior and 8.0.17 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

1.52 CVE-2021-2352

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 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

1.53 CVE-2020-14837

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.54 CVE-2020-14867

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior

and 8.0.21 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 3.1 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: 6.8

1.55 CVE-2021-2081

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 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 3.1 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

1.56 CVE-2021-2070

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.57 CVE-2020-14888

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.58 CVE-2020-14868

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.59 CVE-2020-14891

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.60 CVE-2021-2055

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.61 CVE-2021-2012

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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

1.62 CVE-2021-2021

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.63 CVE-2021-2024

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.64 CVE-2020-14765

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 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

1.65 CVE-2020-14845

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.66 CVE-2021-2046

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior.

Easily exploitable vulnerability allows high 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 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).

CVSS: 6.8

1.67 CVE-2021-2009

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.19 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

1.68 CVE-2021-2058

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 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 3.1 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

1.69 CVE-2020-14809

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.70 CVE-2020-14678

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS: 6.5

1.71 CVE-2020-14663

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS: 6.5

1.72 CVE-2021-2144

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A

CVSS: 6.5

1.73 CVE-2022-21368

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 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 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 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).

CVSS: 6.5

1.74 CVE-2020-14697

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS: 6.5

1.75 CVE-2020-14828

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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 takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

CVSS: 6.5

1.76 CVE-2021-2038

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 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 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: 6.3

1.77 CVE-2021-2006

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows low 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. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.3

1.78 CVE-2021-2022

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and

8.0.22 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 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: 6.3

1.79 CVE-2021-2056

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 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 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: 6.3

1.80 CVE-2021-2061

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 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 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: 6.3

1.81 CVE-2022-21254

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.3

1.82 CVE-2018-3185

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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 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

1.83 CVE-2020-14651

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 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: 5.5

1.84 CVE-2020-14643

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 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: 5.5

1.85 CVE-2019-2534

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I

CVSS: 5.5

1.86 CVE-2019-2819

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 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 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

1.87 CVE-2018-3187

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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 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

1.88 CVE-2018-3064

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 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: 5.5

1.89 CVE-2018-3247

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 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 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/

CVSS: 5.5

1.90 CVE-2021-2304

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 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: 5.5

1.91 CVE-2020-2760

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.29 and prior and 8.0.19 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 3.0 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

1.92 CVE-2021-35612

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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: 5.5

1.93 CVE-2022-21479

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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 and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H).

CVSS: 5.5

1.94 CVE-2019-2758

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). 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 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

1.95 CVE-2019-2436

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.13 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 3.0 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

1.96 CVE-2019-2778

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 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

1.97 CVE-2022-21265

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 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 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).

CVSS: 5.5

1.98 CVE-2018-3060

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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 creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).

CVSS: 5.5

1.99 CVE-2019-2791

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). 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 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 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).

CVSS: 5.5

1.100 CVE-2022-21425

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 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 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: 5.5

1.101 CVE-2019-2800

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.16 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: 5.5

1.102 CVE-2018-3195

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 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 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

1.103 CVE-2021-1998

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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 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 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).
CVSS: 5.5

1.104 CVE-2022-21478

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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 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: 5.5

1.105 CVE-2019-2991

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.017 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 3.0 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

1.106 CVE-2022-21351

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 5.5

1.107 CVE-2021-35610

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 5.5

1.108 CVE-2022-21367

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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: 5.5

1.109 CVE-2022-21378

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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: 5.5

1.110 CVE-2022-21301

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 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: 5.5

1.111 CVE-2022-21278

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 5.5

1.112 CVE-2019-2822

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Admin / InnoDB Cluster). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows unauthenticated 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 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).

CVSS: 5.1

1.113 CVE-2020-5258

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: In affected versions of dojo (NPM package), the deepCopy method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. This has been patched in versions 1.12.8, 1.13.7, 1.14.6, 1.15.3 and 1.16.2

CVSS: 5.0

1.114 CVE-2020-11080

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.

CVSS: 5.0

1.115 CVE-2019-2920

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 5.3.13 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial

of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVSS: 5.0

1.116 CVE-2020-11655

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.

CVSS: 5.0

1.117 CVE-2019-2632

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

CVSS: 5.0

1.118 CVE-2020-1967

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.119 CVE-2018-3171

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 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 as well as unauthorized update, insert or delete access to some of MySQL Server 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

1.120 CVE-2021-2010

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).

CVSS: 4.9

1.121 CVE-2022-21352

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H).

CVSS: 4.9

1.122 CVE-2018-3081

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.123 CVE-2021-2088

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable 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 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.9

1.124 CVE-2021-2087

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable 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 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.9

1.125 CVE-2021-35602

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 4.9

1.126 CVE-2020-2768

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.3.28 and prior, 7.4.27 and prior, 7.5.17 and prior, 7.6.13 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. 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 Cluster as well as unauthorized update, insert or delete access to some of MySQL Cluster accessible data. CVSS 3.0 Base Score 6.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H).

CVSS: 4.9

1.127 CVE-2021-2356

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.128 CVE-2022-21316

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.6

1.129 CVE-2022-21318

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.6

1.130 CVE-2020-1971

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.131 CVE-2019-16168

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: In SQLite through 3.29.0, whereLoopAddBtreeIndex in sqlite3.c can crash a browser or other application because of missing validation of a sqlite_stat1 sz field, aka a "severe division by zero in the query planner."

CVSS: 4.3

1.132 CVE-2021-2007

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.3

1.133 CVE-2019-1559

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application

must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVSS: 4.3

1.134 CVE-2018-3123

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVSS: 4.3

1.135 CVE-2020-2570

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated 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. 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

1.136 CVE-2020-2573

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated 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. 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

1.137 CVE-2020-2574

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated 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. 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

1.138 CVE-2018-3144

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 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

1.139 CVE-2020-2804

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 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

1.140 CVE-2018-0735

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
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

1.141 CVE-2020-2922

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client 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/A:N).
CVSS: 4.3

1.142 CVE-2020-14591

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.20 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 3.1 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: 4.0

1.143 CVE-2019-2494

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 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-2020-14614

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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

1.145 CVE-2020-14620

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 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

1.146 CVE-2019-2495

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 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-2019-2747

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 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

1.148 CVE-2020-14624

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.20 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-2020-14632

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 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

1.150 CVE-2019-2755

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.151 CVE-2020-14634

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.152 CVE-2018-3156

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.153 CVE-2019-2757

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.154 CVE-2020-14641

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).

CVSS: 4.0

1.155 CVE-2020-14654

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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

1.156 CVE-2020-14656

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.20 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

1.157 CVE-2019-2507

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.158 CVE-2020-14680

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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 3.1 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: 4.0

1.159 CVE-2020-14702

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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

1.160 CVE-2019-2510

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.161 CVE-2019-2784

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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

1.162 CVE-2020-14725

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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

1.163 CVE-2020-14769

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 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: 4.0

1.164 CVE-2018-3078

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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

1.165 CVE-2020-14773

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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: 4.0

1.166 CVE-2020-14776

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 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: 4.0

1.167 CVE-2022-21339

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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

1.168 CVE-2020-14777

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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: 4.0

1.169 CVE-2019-2528

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.170 CVE-2019-2795

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 8.0.16 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

1.171 CVE-2020-14785

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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: 4.0

1.172 CVE-2020-14789

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 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: 4.0

1.173 CVE-2018-3182

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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

1.174 CVE-2019-2529

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.175 CVE-2020-14794

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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: 4.0

1.176 CVE-2019-2530

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.13 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

1.177 CVE-2020-14799

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.20 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

1.178 CVE-2020-14800

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). 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: 4.0

1.179 CVE-2020-14804

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). 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: 4.0

1.180 CVE-2019-2531

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.181 CVE-2019-2802

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.182 CVE-2019-2803

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.183 CVE-2020-14827

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).

CVSS: 4.0

1.184 CVE-2019-2532

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.185 CVE-2019-2805

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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

1.186 CVE-2019-2808

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.187 CVE-2019-2810

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.188 CVE-2020-14838

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C

CVSS: 4.0

1.189 CVE-2018-3186

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.190 CVE-2019-2811

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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

1.191 CVE-2019-2812

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 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

1.192 CVE-2018-3080

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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

1.193 CVE-2022-21309

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.194 CVE-2022-21337

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.195 CVE-2022-21335

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.196 CVE-2022-21342

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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

1.197 CVE-2019-2815

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.198 CVE-2020-14860

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.199 CVE-2019-2537

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.200 CVE-2019-2826

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 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

1.201 CVE-2020-14893

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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: 4.0

1.202 CVE-2019-2539

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 8.0.13 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

1.203 CVE-2019-2879

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.204 CVE-2018-3200

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.205 CVE-2022-21344

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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

1.206 CVE-2019-2911

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.207 CVE-2019-2914

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.27 and prior and 8.0.17 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

1.208 CVE-2018-3203

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.209 CVE-2021-2019

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.19 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.210 CVE-2019-2946

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.27 and prior and 8.0.17 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

1.211 CVE-2019-2566

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). 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

1.212 CVE-2019-2948

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: 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

1.213 CVE-2021-2032

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.214 CVE-2019-2580

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.215 CVE-2019-2957

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.17 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

1.216 CVE-2019-2581

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). 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

1.217 CVE-2019-2960

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.27 and prior and 8.0.17 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

1.218 CVE-2018-3082

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A

CVSS: 4.0

1.219 CVE-2018-3212

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 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

1.220 CVE-2019-2963

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 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

1.221 CVE-2019-2966

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 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

1.222 CVE-2019-2584

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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

1.223 CVE-2019-2967

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 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

1.224 CVE-2018-3065

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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

1.225 CVE-2019-2968

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 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

1.226 CVE-2019-2585

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.227 CVE-2019-2974

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 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

1.228 CVE-2019-2587

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 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

1.229 CVE-2019-2982

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 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

1.230 CVE-2021-2146

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.231 CVE-2021-2160

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.17 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

1.232 CVE-2018-3251

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.233 CVE-2019-2589

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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

1.234 CVE-2021-2162

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.235 CVE-2021-2166

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.236 CVE-2019-2998

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 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

1.237 CVE-2021-2170

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.238 CVE-2021-2172

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 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 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: 4.0

1.239 CVE-2020-14553

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 5.7.30 and prior and 8.0.20 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.240 CVE-2019-2593

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.241 CVE-2021-2178

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 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 3.1 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: 4.0

1.242 CVE-2021-2180

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.243 CVE-2019-3011

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 8.0.17 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

1.244 CVE-2021-2194

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.245 CVE-2021-2201

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 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

1.246 CVE-2022-21374

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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

1.247 CVE-2019-2455

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.248 CVE-2020-14559

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.249 CVE-2018-3133

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.250 CVE-2018-3277

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.251 CVE-2021-2202

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 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 3.1 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: 4.0

1.252 CVE-2021-2203

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.253 CVE-2020-14586

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 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

1.254 CVE-2018-3170

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.255 CVE-2020-14597

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 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

1.256 CVE-2018-3077

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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

1.257 CVE-2020-14619

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.20 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 3.1 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: 4.0

1.258 CVE-2019-2746

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Data Dictionary). Supported versions that are affected are 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

1.259 CVE-2020-14623

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 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

1.260 CVE-2020-2925

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.19 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

1.261 CVE-2020-14631

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Audit). Supported versions that are affected are 8.0.20 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

1.262 CVE-2019-2752

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 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

1.263 CVE-2020-14633

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A

CVSS: 4.0

1.264 CVE-2019-2502

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.13 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

1.265 CVE-2021-2212

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.266 CVE-2019-2774

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.267 CVE-2021-2213

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 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 3.1 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

1.268 CVE-2021-2215

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 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

1.269 CVE-2021-2226

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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 access to critical data or complete access

to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).

CVSS: 4.0

1.270 CVE-2018-3137

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.271 CVE-2018-3278

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 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

1.272 CVE-2020-2577

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.18 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

1.273 CVE-2019-2780

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Components / Services). Supported versions that are affected are 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

1.274 CVE-2018-3173

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.275 CVE-2019-2785

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.276 CVE-2019-2789

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.277 CVE-2021-2293

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 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

1.278 CVE-2020-14775

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 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: 4.0

1.279 CVE-2020-2580

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 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

1.280 CVE-2021-2299

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.281 CVE-2019-2688

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.282 CVE-2020-14786

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). 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: 4.0

1.283 CVE-2019-2796

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.284 CVE-2020-14790

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.31 and prior and 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: 4.0

1.285 CVE-2018-3079

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.11 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

1.286 CVE-2020-14793

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 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: 4.0

1.287 CVE-2019-2798

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.288 CVE-2021-2301

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.289 CVE-2018-3279

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 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

1.290 CVE-2020-2588

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.18 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

1.291 CVE-2021-2305

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 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

1.292 CVE-2019-2801

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 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

1.293 CVE-2021-2308

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.294 CVE-2020-2627

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.18 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

1.295 CVE-2021-2340

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 4.0

1.296 CVE-2022-21370

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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

1.297 CVE-2020-2660

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.28 and prior and 8.0.18 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

1.298 CVE-2019-2624

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.299 CVE-2020-2679

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 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

1.300 CVE-2021-2357

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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

1.301 CVE-2019-2533

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 8.0.13 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVSS: 4.0

1.302 CVE-2021-2479

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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

1.303 CVE-2019-2625

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.304 CVE-2021-2481

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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: 4.0

1.305 CVE-2021-35575

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.306 CVE-2018-3075

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.11 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

1.307 CVE-2022-21327

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.308 CVE-2019-2626

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.309 CVE-2021-35577

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior.

Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protcol 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

1.310 CVE-2021-35591

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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

1.311 CVE-2021-35597

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low 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. 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: 4.0

1.312 CVE-2019-2627

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 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

1.313 CVE-2021-35607

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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: 4.0

1.314 CVE-2019-2628

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). 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

1.315 CVE-2020-14547

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.20 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

1.316 CVE-2020-2759

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.19 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

1.317 CVE-2021-35622

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 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

1.318 CVE-2021-35624

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).

CVSS: 4.0

1.319 CVE-2020-2761

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 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

1.320 CVE-2021-35626

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.321 CVE-2021-35628

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.322 CVE-2022-21454

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.37 and prior and 8.0.28 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: 4.0

1.323 CVE-2019-2631

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 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

1.324 CVE-2020-2763

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 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

1.325 CVE-2021-35630

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).

CVSS: 4.0

1.326 CVE-2020-2765

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.29 and prior and 8.0.19 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

1.327 CVE-2021-35633

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 4.0

1.328 CVE-2021-35634

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.329 CVE-2021-35636

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.330 CVE-2018-3073

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.11 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

1.331 CVE-2018-3285

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Windows). Supported versions that are affected are 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

1.332 CVE-2020-2774

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 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

1.333 CVE-2021-35641

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.334 CVE-2020-2780

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 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. 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

1.335 CVE-2021-35643

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.336 CVE-2021-35645

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.337 CVE-2020-14539

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and

prior and 8.0.20 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 3.1 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: 4.0

1.338 CVE-2022-21336

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.339 CVE-2018-3054

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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

1.340 CVE-2018-3286

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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 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

1.341 CVE-2020-2812

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 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

1.342 CVE-2021-35647

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.343 CVE-2019-2950

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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

1.344 CVE-2022-21245

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.345 CVE-2020-2853

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 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

1.346 CVE-2022-21249

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 4.0

1.347 CVE-2020-2892

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.348 CVE-2019-2681

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.349 CVE-2020-2893

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 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

1.350 CVE-2022-21264

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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

1.351 CVE-2022-21270

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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

1.352 CVE-2020-2896

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.19 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

1.353 CVE-2022-21280

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.354 CVE-2022-21285

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.355 CVE-2019-2420

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.356 CVE-2019-2685

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.357 CVE-2020-2898

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). The supported version that is affected is 8.0.19. 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

1.358 CVE-2022-21287

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.359 CVE-2022-21289

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.360 CVE-2020-2903

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.19 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

1.361 CVE-2022-21297

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.362 CVE-2021-2164

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.363 CVE-2019-2997

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 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

1.364 CVE-2021-2169

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.365 CVE-2019-2592

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). 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

1.366 CVE-2019-3003

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 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

1.367 CVE-2018-3276

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 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

1.368 CVE-2019-3004

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*
Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.17 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

1.369 CVE-2022-21356

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.370 CVE-2021-2179

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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

1.371 CVE-2019-3009

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection). Supported versions that are affected are 8.0.17 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: 4.0

1.372 CVE-2021-2193

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.373 CVE-2019-2596

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.374 CVE-2021-2196

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 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

1.375 CVE-2019-2606

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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

1.376 CVE-2022-21307

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows

high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.377 CVE-2020-2904

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.378 CVE-2021-2208

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 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

1.379 CVE-2020-2572

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plugin). Supported versions that are affected are 5.7.28 and prior and 8.0.18 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.380 CVE-2019-2607

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.381 CVE-2022-21303

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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

1.382 CVE-2019-2687

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.383 CVE-2022-21304

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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

1.384 CVE-2021-2217

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 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

1.385 CVE-2021-2230

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.386 CVE-2019-2694

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 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

1.387 CVE-2021-2278

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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

1.388 CVE-2020-2579

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 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

1.389 CVE-2021-2298

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 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 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: 4.0

1.390 CVE-2018-3067

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.11 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

1.391 CVE-2021-2300

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 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

1.392 CVE-2019-2620

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 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

1.393 CVE-2022-21308

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.394 CVE-2020-2589

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.17 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

1.395 CVE-2018-3280

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: JSON). Supported versions that are affected are 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

1.396 CVE-2020-2923

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.397 CVE-2022-21310

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.398 CVE-2018-3143

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.399 CVE-2020-2924

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.400 CVE-2022-21489

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.401 CVE-2022-21417

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.402 CVE-2022-21412

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 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

1.403 CVE-2019-2689

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.404 CVE-2022-21314

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.405 CVE-2022-21348

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 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

1.406 CVE-2021-2478

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 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

1.407 CVE-2020-2686

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 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

1.408 CVE-2018-3282

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.409 CVE-2021-35546

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 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

1.410 CVE-2021-35596

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 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

1.411 CVE-2022-21315

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.412 CVE-2019-2691

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 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

1.413 CVE-2020-2928

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.414 CVE-2019-2482

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.415 CVE-2022-21320

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover

of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.416 CVE-2022-21372

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 4.0

1.417 CVE-2019-2693

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 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

1.418 CVE-2022-21322

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.419 CVE-2021-35623

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A

CVSS: 4.0

1.420 CVE-2021-35625

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 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 read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

CVSS: 4.0

1.421 CVE-2018-3161

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 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

1.422 CVE-2021-35627

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.423 CVE-2020-2762

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 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

1.424 CVE-2021-35629

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 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

1.425 CVE-2019-2481

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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

1.426 CVE-2022-21326

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.427 CVE-2021-35631

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 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

1.428 CVE-2018-3145

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 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

1.429 CVE-2022-21328

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.430 CVE-2021-35635

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.431 CVE-2020-2770

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.18 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

1.432 CVE-2022-21329

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.433 CVE-2019-2695

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 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

1.434 CVE-2020-14540

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 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

1.435 CVE-2022-21330

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.436 CVE-2021-35640

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C

CVSS: 4.0

1.437 CVE-2020-2779

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 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

1.438 CVE-2021-35642

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.439 CVE-2019-2635

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 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

1.440 CVE-2021-35644

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.441 CVE-2021-35646

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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

1.442 CVE-2021-35648

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 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

1.443 CVE-2020-2814

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.47 and prior, 5.7.28 and prior and 8.0.18 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

1.444 CVE-2019-2644

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.445 CVE-2022-21332

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.446 CVE-2018-3162

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 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

1.447 CVE-2022-21334

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.448 CVE-2022-21358

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 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: 4.0

1.449 CVE-2022-21362

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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

1.450 CVE-2018-3056

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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

1.451 CVE-2020-2895

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 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

1.452 CVE-2022-21279

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.453 CVE-2019-2683

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.6.43 and prior, 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

1.454 CVE-2022-21284

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS

3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.455 CVE-2020-2897

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.456 CVE-2022-21286

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.457 CVE-2018-3155

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 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. 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

1.458 CVE-2022-21288

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24

and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.459 CVE-2020-2901

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 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

1.460 CVE-2022-21290

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.461 CVE-2019-2686

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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

1.462 CVE-2020-14567

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 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

1.463 CVE-2019-2434

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.464 CVE-2022-21483

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.465 CVE-2019-2486

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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

1.466 CVE-2020-14568

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 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

1.467 CVE-2020-14575

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 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

1.468 CVE-2019-2737

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 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

1.469 CVE-2022-21482

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

CVSS: 4.0

1.470 CVE-2022-21427

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). 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

1.471 CVE-2019-2740

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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

1.472 CVE-2020-14576

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 5.7.30 and prior and 8.0.20 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 3.1 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: 4.0

1.473 CVE-2019-2503

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the 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 and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).

CVSS: 3.8

1.474 CVE-2019-2739

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 3.6

1.475 CVE-2019-2741

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

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

1.476 CVE-2019-2743

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 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

1.477 CVE-2020-14771

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 partial denial of service

(partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 3.5

1.478 CVE-2013-1548

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.1.63 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Types.

CVSS: 3.5

1.479 CVE-2020-14791

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

CVSS: 3.5

1.480 CVE-2018-3062

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached 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

1.481 CVE-2019-2814

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 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. CVSS 3.0 Base Score 2.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N).

CVSS: 3.5

1.482 CVE-2019-2938

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.27 and prior and 8.0.17 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

1.483 CVE-2019-2993

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 5.7.27 and prior and 8.0.17 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

1.484 CVE-2021-2171

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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: 3.5

1.485 CVE-2021-2174

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 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: 3.5

1.486 CVE-2019-3018

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 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

1.487 CVE-2019-2614

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 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

1.488 CVE-2019-2617

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 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

1.489 CVE-2020-2584

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.28 and prior and 8.0.18 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).

CVSS: 3.5

1.490 CVE-2019-2623

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 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

1.491 CVE-2020-2694

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.18 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

1.492 CVE-2018-3283

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Logging). Supported versions that are affected are 5.7.23 and prior and 8.0.12 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

1.493 CVE-2020-2752

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low 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. 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

1.494 CVE-2021-35608

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 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 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.495 CVE-2018-3284

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 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

1.496 CVE-2019-2630

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 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

1.497 CVE-2019-2636

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Procotol 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

1.498 CVE-2022-21302

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 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 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.499 CVE-2020-2921

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.19 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

1.500 CVE-2018-3074

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.11 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

1.501 CVE-2020-2926

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.19 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

1.502 CVE-2020-2930

!–> CVE for cpe:2.3:a:oracle:mysql:8.0.3:::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.19 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

1.503 CVE-2011-0411

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: The STARTTLS implementation in Postfix 2.4.x before 2.4.16, 2.5.x before 2.5.12, 2.6.x before 2.6.9, and 2.7.x before 2.7.3 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack.

CVSS: 6.8

1.504 CVE-2011-1720

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: The SMTP server in Postfix before 2.5.13, 2.6.x before 2.6.10, 2.7.x before 2.7.4, and 2.8.x before 2.8.3, when certain Cyrus SASL authentication methods are enabled, does not create a new server handle after client authentication fails, which allows remote attackers to cause a denial of service (heap memory corruption and daemon crash) or possibly execute arbitrary code via an invalid AUTH command with one method followed by an AUTH command with a different method.

CVSS: 6.8

1.505 CVE-2017-10140

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.

CVSS: 4.6

1.506 CVE-2008-3889

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application

slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.

CVSS: 2.1

1.507 CVE-2023-51764

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::::*

Summary: Postfix through 3.8.5 allows SMTP smuggling unless configured with smtpd_data_restrictions=reject_unauth_pipelining and smtpd_discard_ehlo_keywords=chunking (or certain other options that exist in recent versions). Remote attackers can use a published exploitation technique to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This occurs because Postfix supports . but some other popular e-mail servers do not. To prevent attack variants (by always disallowing without), a different solution is required, such as the smtpd_forbid_bare_newline=yes option with a Postfix minimum version of 3.5.23, 3.6.13, 3.7.9, 3.8.4, or 3.9.

CVSS: N/A