Vulnerability Discovery Results

Sunday 7th July, 2024

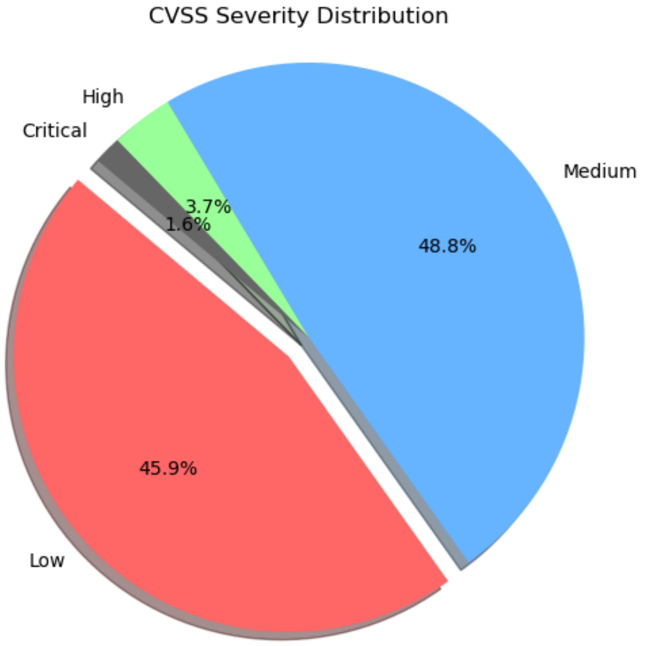
15:09

(UTC+2, PARIS)

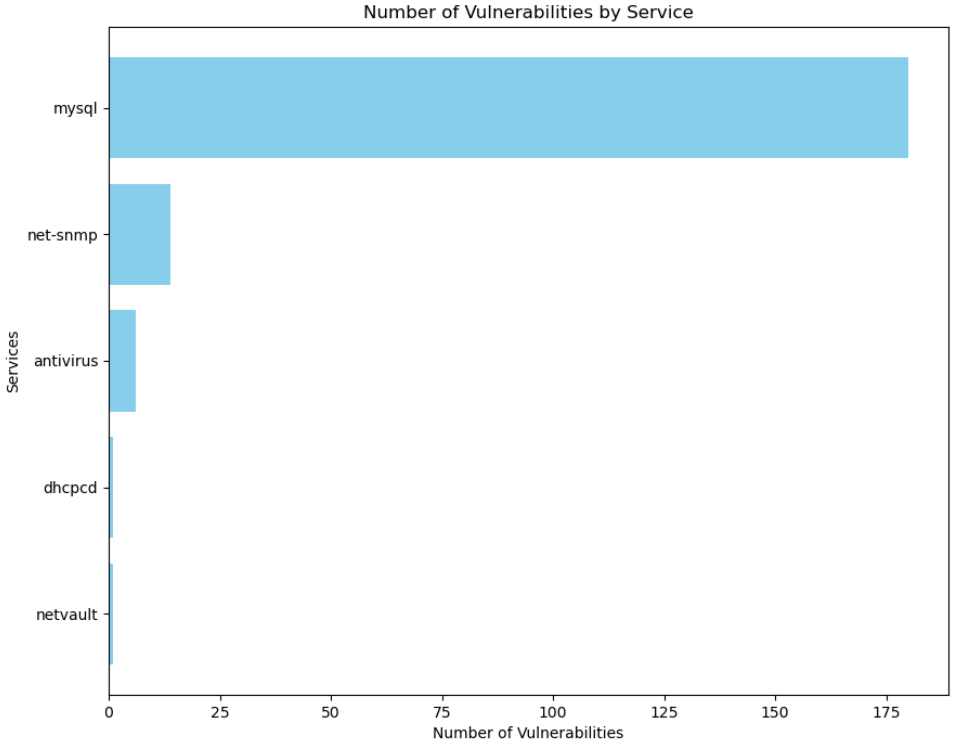
Company Name	First Name	Last Name
VSCodium	Trish	Terese

Name	OS Name	OS SP
nestie_louna	Linux	1.15.X

CVE	Critical Severity
CVE-2009-1429	10.0
CVE-2009-1430	9.3
CVE-2010-0111	9.3
CVE-2011-0688	9.3



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2009-4484

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL connection and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflow1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: this was originally reported for MySQL 5.0.51a.

CVSS: 7.5

1.2 CVE-2020-14760

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 7.5

1.3 CVE-2013-2395

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.8

1.4 CVE-2013-5860

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.8

1.5 CVE-2013-5882

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.8

1.6 CVE-2016-0504

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.8

1.7 CVE-2016-3518

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.8

1.8 CVE-2020-14814

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.9 CVE-2020-14830

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.10 CVE-2020-14837

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.11 CVE-2020-14839

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.12 CVE-2020-14845

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.13 CVE-2020-14846

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.14 CVE-2020-14852

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.15 CVE-2012-4414

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: Multiple SQL injection vulnerabilities in the replication code in Oracle MySQL possibly before 5.5.29, and MariaDB 5.1.x through 5.1.62, 5.2.x through 5.2.12, 5.3.x through 5.3.7, and 5.5.x through 5.5.25, allow remote authenticated users to execute arbitrary SQL commands via vectors related to the binary log. NOTE: as of 20130116, Oracle has not commented on claims from a downstream vendor that the fix in MySQL 5.5.29 is incomplete.

CVSS: 6.5

1.16 CVE-2014-2444

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.5

1.17 CVE-2014-2484

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.5

1.18 CVE-2015-2617

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 6.5

1.19 CVE-2012-3147

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote attackers to affect integrity and availability, related to MySQL Client.

CVSS: 6.4

1.20 CVE-2013-3798

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 5.8

1.21 CVE-2017-3454

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 5.5

1.22 CVE-2017-3455

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 5.5

1.23 CVE-2019-2731

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 5.5

1.24 CVE-2013-1570

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 5.0

1.25 CVE-2020-1967

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.26 CVE-2016-3588

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.9

1.27 CVE-2021-2356

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.28 CVE-2014-0433

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.3

1.29 CVE-2016-0594

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.3

1.30 CVE-2015-3152

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.3

1.31 CVE-2017-3467

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/

CVSS: 4.3

1.32 CVE-2017-3650

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/

CVSS: 4.3

1.33 CVE-2018-0735

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

1.34 CVE-2020-1971

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.35 CVE-2007-2583

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: The in_decimal::set function in item_cmpfunc.cc in MySQL before 5.0.40, and 5.1 before 5.1.18-beta, allows context-dependent attackers to cause a denial of service (crash) via a crafted IF clause that results in a divide-by-zero error and a NULL pointer dereference.

CVSS: 4.0

1.36 CVE-2012-0583

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.60 and earlier, and 5.5.19 and earlier, allows remote authenticated users to affect availability, related to MyISAM.

CVSS: 4.0

1.37 CVE-2012-1696

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.19 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.

CVSS: 4.0

1.38 CVE-2012-3144

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.

CVSS: 4.0

1.39 CVE-2013-3795

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.40 CVE-2013-3796

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.41 CVE-2013-3806

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.42 CVE-2013-3807

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.43 CVE-2013-5767

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.44 CVE-2013-5786

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.45 CVE-2013-5894

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.46 CVE-2013-5881

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.47 CVE-2014-2434

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.48 CVE-2014-2435

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.49 CVE-2014-2442

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.50 CVE-2014-2450

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.51 CVE-2014-4233

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.52 CVE-2014-4238

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.53 CVE-2015-0409

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.54 CVE-2015-0405

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.55 CVE-2015-0423

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.56 CVE-2015-0438

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.57 CVE-2015-0439

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.58 CVE-2015-0500

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.59 CVE-2015-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.60 CVE-2015-0508

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.61 CVE-2015-2611

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.62 CVE-2015-4756

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.63 CVE-2015-4772

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.64 CVE-2015-4730

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.65 CVE-2015-4800

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.66 CVE-2015-4833

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.67 CVE-2015-4862

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.68 CVE-2015-4904

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

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

CVSS: 4.0

1.69 CVE-2015-4905

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

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

CVSS: 4.0

1.70 CVE-2016-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

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

CVSS: 4.0

1.71 CVE-2016-0595

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

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

CVSS: 4.0

1.72 CVE-2016-0611

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

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

CVSS: 4.0

1.73 CVE-2016-0616

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.74 CVE-2016-3424

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.75 CVE-2016-3440

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.76 CVE-2016-5436

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.77 CVE-2016-5437

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.78 CVE-2016-5441

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.79 CVE-2016-5442

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.80 CVE-2016-5628

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.81 CVE-2016-5631

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.82 CVE-2016-5632

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

Summary: Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.

CVSS: 4.0

1.83 CVE-2016-5633

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-8290.

CVSS: 4.0

1.84 CVE-2016-5634

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.85 CVE-2016-5635

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.86 CVE-2017-3251

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.87 CVE-2017-3256

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.88 CVE-2017-3452

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.89 CVE-2017-3457

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.90 CVE-2017-3458

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 4.0

1.91 CVE-2017-3459

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.92 CVE-2017-3460

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.93 CVE-2017-3465

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.94 CVE-2017-3638

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.95 CVE-2017-3639

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.96 CVE-2017-3640

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.97 CVE-2017-3642

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.98 CVE-2017-3643

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 4.0

1.99 CVE-2017-3644

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.100 CVE-2017-3645

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.101 CVE-2017-3646

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.102 CVE-2017-10165

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.103 CVE-2017-10167

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.104 CVE-2017-10284

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.105 CVE-2017-10296

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.106 CVE-2017-10311

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 4.0

1.107 CVE-2017-10313

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.108 CVE-2018-3061

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.109 CVE-2018-3071

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 4.0

1.110 CVE-2019-2755

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.111 CVE-2019-2757

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

1.112 CVE-2022-21417

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

1.113 CVE-2014-4240

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.6

1.114 CVE-2010-2008

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

Summary: MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGRADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the server data directory.

CVSS: 3.5

1.115 CVE-2012-3149

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect confidentiality, related to MySQL Client.

CVSS: 3.5

1.116 CVE-2012-3156

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.

CVSS: 3.5

1.117 CVE-2013-1566

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.118 CVE-2013-1567

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.119 CVE-2013-2381

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.120 CVE-2013-3810

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.121 CVE-2013-3811

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.122 CVE-2013-5793

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.123 CVE-2014-0427

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.124 CVE-2014-0431

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.125 CVE-2014-2451

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.126 CVE-2015-0385

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.127 CVE-2015-0506

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.128 CVE-2015-0507

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.129 CVE-2015-2567

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.130 CVE-2015-2639

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.131 CVE-2015-2641

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.132 CVE-2015-4761

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.133 CVE-2015-4769

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4767.

CVSS: 3.5

1.134 CVE-2015-4771

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.135 CVE-2015-4791

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.136 CVE-2015-4890

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.137 CVE-2016-0610

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.138 CVE-2016-0652

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.139 CVE-2016-0653

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.140 CVE-2016-0654

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.141 CVE-2016-0656

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.142 CVE-2016-0657

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.143 CVE-2016-0658

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.144 CVE-2016-0659

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.145 CVE-2016-0662

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.146 CVE-2016-0663

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:::::

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

CVSS: 3.5

1.147 CVE-2016-8286

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.148 CVE-2016-8287

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.149 CVE-2016-8290

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.150 CVE-2017-3319

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.151 CVE-2017-3320

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*:*

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

CVSS: 3.5

1.152 CVE-2017-3468

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 3.5

1.153 CVE-2017-3529

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 3.5

1.154 CVE-2017-3637

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 3.5

1.155 CVE-2019-2741

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

1.156 CVE-2014-4214

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 3.3

1.157 CVE-2016-8289

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 3.3

1.158 CVE-2014-0430

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 2.8

1.159 CVE-2015-0511

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 2.8

1.160 CVE-2015-2566

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 2.8

1.161 CVE-2016-0607

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: 2.8

1.162 CVE-2016-0667

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 2.8

1.163 CVE-2019-7317

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.

CVSS: 2.6

1.164 CVE-2012-4452

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: MySQL 5.0.88, and possibly other versions and platforms, allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of a CVE-2009-4030 regression, which was not omitted in other packages and versions such as MySQL 5.0.95 in Red Hat Enterprise Linux 6.

CVSS: 2.1

1.165 CVE-2013-5770

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 2.1

1.166 CVE-2015-2661

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 2.1

1.167 CVE-2015-4910

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 2.1

1.168 CVE-2020-15358

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

CVSS: 2.1

1.169 CVE-2021-22570

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

Summary: Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

CVSS: 2.1

1.170 CVE-2022-21444

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 2.1

1.171 CVE-2015-4766

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 1.9

1.172 CVE-2015-0498

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 1.7

1.173 CVE-2015-4767

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 1.7

1.174 CVE-2016-5443

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: 1.2

1.175 CVE-2023-21977

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: N/A

1.176 CVE-2023-21980

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: N/A

1.177 CVE-2023-22007

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a:*:*:*:*:*:*

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

CVSS: N/A

1.178 CVE-2023-22015

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: N/A

1.179 CVE-2023-22026

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: N/A

1.180 CVE-2023-22028

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.24:a::::::

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

CVSS: N/A

1.181 CVE-2002-1403

!–> CVE for cpe:2.3:a:phystech:dhcpcd:1.3.22_pl1:::::::*

Summary: dhcpcd DHCP client daemon 1.3.22 and earlier allows local users to execute arbitrary code via shell metacharacters that are fed from a dhcpd .info script into a .exe script.

CVSS: 7.2

1.182 CVE-2007-5846

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: The SNMP agent (snmp_agent.c) in net-snmp before 5.4.1 allows remote attackers to cause a denial of service (CPU and memory consumption) via a GETBULK request with a large max-repeaters value.

CVSS: 7.8

1.183 CVE-2006-6305

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: Unspecified vulnerability in Net-SNMP 5.3 before 5.3.0.1, when configured using the rocommunity or rouser snmpd.conf tokens, causes Net-SNMP to grant write access to users or communities that only have read-only access.

CVSS: 7.5

1.184 CVE-2015-5621

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

CVSS: 7.5

1.185 CVE-2020-15861

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.

CVSS: 7.2

1.186 CVE-2020-15862

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: Net-SNMP through 5.8 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.

CVSS: 7.2

1.187 CVE-2008-6123

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:::::::*

Summary: The netsnmp_udp_fmtaddr function (snmplib/snmpUDPDomain.c) in net-snmp 5.0.9 through 5.4.2.1, when using TCP wrappers for client authorization, does not properly parse hosts.allow rules, which allows remote attackers to bypass intended access restrictions and execute SNMP queries, related to "source/destination IP address confusion."

CVSS: 5.0

1.188 CVE-2014-2310

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: The AgentX subagent in Net-SNMP before 5.4.4 allows remote attackers to cause a denial of service (hang) by sending a multi-object request with an Object ID (OID) containing more subids than previous requests, a different vulnerability than CVE-2012-6151.

CVSS: 5.0

1.189 CVE-2014-3565

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: snmplib/mib.c in net-snmp 5.7.0 and earlier, when the -OQ option is used, allows remote attackers to cause a denial of service (snmptrapd crash) via a crafted SNMP trap message, which triggers a conversion to the variable type designated in the MIB file, as demonstrated by a NULL type in an ifMtu trap message.

CVSS: 5.0

1.190 CVE-2018-18066

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

CVSS: 5.0

1.191 CVE-2012-6151

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: Net-SNMP 5.7.1 and earlier, when AgentX is registering to handle a MIB and processing GETNEXT requests, allows remote attackers to cause a denial of service (crash or infinite loop, CPU consumption, and hang) by causing the AgentX subagent to timeout.

CVSS: 4.3

1.192 CVE-2014-2285

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: The perl_trapd_handler function in perl/TrapReceiver/TrapReceiver.xs in Net-SNMP 5.7.3.pre3 and earlier, when using certain Perl versions, allows remote attackers to cause a denial of service (snmptrapd crash) via an empty community string in an SNMP trap, which triggers a NULL pointer dereference within the newSVpv function in Perl.

CVSS: 4.3

1.193 CVE-2018-18065

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: _set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

CVSS: 4.0

1.194 CVE-2019-20892

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.

CVSS: 4.0

1.195 CVE-2015-8100

!–> CVE for cpe:2.3:a:net-snmp:net-snmp:5.3:*:*:*:*:*:*:*

Summary: The net-snmp package in OpenBSD through 5.8 uses 0644 permissions for snmpd.conf, which allows local users to obtain sensitive community information by reading this file.

CVSS: 2.1

1.196 CVE-2009-1429

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: The Intel LANDesk Common Base Agent (CBA) in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allows remote attackers to execute arbitrary commands via a crafted packet whose contents are interpreted as a command to be launched in a new process by the CreateProcessA function.

CVSS: 10.0

1.197 CVE-2009-1430

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: Multiple stack-based buffer overflows in IAO.EXE in the Intel Alert Originator Service in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allow remote attackers to execute arbitrary code via (1) a crafted packet or (2) data that ostensibly arrives from the MsgSys.exe process.

CVSS: 9.3

1.198 CVE-2010-0111

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: HDNLRSVC.EXE in the Intel Alert Handler service (aka Symantec Intel Handler service) in Intel Alert Management System (aka AMS or AMS2), as used in Symantec AntiVirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allows remote attackers to execute arbitrary programs by sending msgsys.exe a UNC share pathname, which is used directly in a CreateProcessA (aka CreateProcess) call.

CVSS: 9.3

1.199 CVE-2011-0688

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: Intel Alert Management System (aka AMS or AMS2), as used in Symantec Antivirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allows remote attackers to execute arbitrary commands via crafted messages over TCP, as discovered by Junaid Bohio, a different vulnerability than CVE-2010-0110 and CVE-2010-0111. NOTE: some of these details are obtained from third party information.

CVSS: 9.3

1.200 CVE-2010-0110

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: Multiple stack-based buffer overflows in Intel Alert Management System (aka AMS or AMS2), as used in Symantec AntiVirus Corporate Edition (SAVCE) 10.x before 10.1 MR10, Symantec System Center (SSC) 10.x, and Symantec Quarantine Server 3.5 and 3.6, allow remote attackers to execute arbitrary code via (1) a long string to msgsys.exe, related to the AMSSendAlertAct function in AMSLIB.dll in the Intel Alert Handler service (aka Symantec Intel Handler service); a long (2) modem string or (3) PIN number to msgsys.exe, related to pagehndl.dll in the Intel Alert Handler service; or (4) a message to msgsys.exe, related to iao.exe in the Intel Alert Originator service.

CVSS: 7.9

1.201 CVE-2007-1793

!–> CVE for cpe:2.3:a:symantec:antivirus:10.0.9:*:corporate:*:*:*:*:*

Summary: SPBBCDrv.sys in Symantec Norton Personal Firewall 2006 9.1.0.33 and 9.1.1.7 does not validate certain arguments before being passed to hooked SSDT function handlers, which allows local users to cause a denial of service (crash) or possibly execute arbitrary code via crafted arguments to the (1) NtCreateMutant and (2) NtOpenEvent functions. NOTE: it was later reported that Norton Internet Security 2008 15.0.0.60, and possibly other versions back to 2006, are also affected.

CVSS: 4.9

1.202 CVE-2009-3448

!–> CVE for cpe:2.3:a:bakbone:netvault:8.22:*:*:*:*:*:*:*

Summary: npvmgr.exe in BakBone NetVault Backup 8.22 Build 29 allows remote attackers to cause a denial of service (daemon crash) via a packet to (1) TCP or (2) UDP port 20031 with a large value in an unspecified size field, which is not properly handled in a malloc operation. NOTE: some of these details are obtained from third party information.

CVSS: 5.0