

McAfee Vulnerability Manager for Databases Update

McAfee DVM Security Update v106

This update includes:

- Updated checks for MySQL, MSSQL and PostgreSQL to detect missing patches
- New configuration checks for MSSQL and MySQL databases
- New checks for MariaDB 10.x database to detect recently reported vulnerabilities

The following CVE's are covered for MariaDB 10.x:

- CVE-2016-0668- Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB.
CVE-2016-0668: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0666- Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to Security: Privileges.
CVE-2016-0666: Fixed in MariaDB 10.0.25
- CVE-2016-0655- Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows local users to affect availability via vectors related to InnoDB.
CVE-2016-0655: Fixed in MariaDB 10.0.25
- CVE-2016-0651- Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows local users to affect availability via vectors related to Optimizer.
CVE-2016-0651: Fixed in MariaDB 10.1.10, MariaDB 10.0.23
- CVE-2016-0650- Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to Replication.
CVE-2016-0650: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0649- Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to PS.
CVE-2016-0649: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0648- Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to PS.
CVE-2016-0648: Fixed in MariaDB 10.0.25

- CVE-2016-0647- Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to FTS.
CVE-2016-0647: Fixed in MariaDB 10.0.25
- CVE-2016-0646 - Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to DML.
CVE-2016-0646: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0644 - Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to DDL.
CVE-2016-0644: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0643 - Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect confidentiality via vectors related to DML.
CVE-2016-0643: Fixed in MariaDB 10.0.25
- CVE-2016-0642 - Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect integrity and availability via vectors related to Federated.
CVE-2016-0642: Fixed in MariaDB 10.1.10, MariaDB 10.0.23
- CVE-2016-0641 - Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect confidentiality and availability via vectors related to MyISAM.
CVE-2016-0641: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0640 - Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect integrity and availability via vectors related to DML.
CVE-2016-0640: Fixed in MariaDB 10.1.12, MariaDB 10.0.24
- CVE-2016-0502- Unspecified vulnerability in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0502: Fixed in MariaDB 10.0.4
- CVE-2015-7744- wolfSSL (formerly CyaSSL) before 3.6.8 does not properly handle faults associated with the Chinese Remainder Theorem (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server, which makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.
CVE-2015-7744: Fixed in MariaDB 10.1.9, MariaDB 10.0.22
- CVE-2015-4913- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors

related to Server : DML, a different vulnerability than CVE-2015-4858.

CVE-2015-4913: Fixed in MariaDB 10.1.8, MariaDB 10.0.22

- CVE-2015-4895- Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.
CVE-2015-4895: Fixed in MariaDB 10.1.8, MariaDB 10.0.21
- CVE-2015-4879- Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to DML.
CVE-2015-4879: Fixed in MariaDB 10.1.8, MariaDB 10.0.21
- CVE-2015-4870- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Parser.
CVE-2015-4870: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4866- 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.
CVE-2015-4866: Fixed in MariaDB 10.1.8, MariaDB 10.0.18
- CVE-2015-4864- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.
CVE-2015-4864: Fixed in MariaDB 10.1.8, MariaDB 10.0.20
- CVE-2015-4861- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.
CVE-2015-4861: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4858- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2015-4913.
CVE-2015-4858: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4836- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : SP.
CVE-2015-4836: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4830- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.
CVE-2015-4830: Fixed in MariaDB 10.1.8, MariaDB 10.0.22

- CVE-2015-4826- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Types.
CVE-2015-4826: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4819- Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client programs.
CVE-2015-4819: Fixed in MariaDB 10.1.8, MariaDB 10.0.21
- CVE-2015-4816- Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.
CVE-2015-4816: Fixed in MariaDB 10.1.8, MariaDB 10.0.21
- CVE-2015-4815- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to Server : DDL.
CVE-2015-4815: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4807- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier, when running on Windows, allows remote authenticated users to affect availability via unknown vectors related to Server : Query Cache.
CVE-2015-4807: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4802- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4792.
CVE-2015-4802: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4792- Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4802.
CVE-2015-4792: Fixed in MariaDB 10.1.8, MariaDB 10.0.22
- CVE-2015-4757- Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier and 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.
CVE-2015-4757: Fixed in MariaDB 10.0.18
- CVE-2015-4752- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to Server : I_S.
CVE-2015-4752: Fixed in MariaDB 10.0.20
- CVE-2015-3152- 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.

CVE-2015-3152: Fixed in MariaDB 10.0.20

- CVE-2015-2648- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2015-2648: Fixed in MariaDB 10.0.20
- CVE-2015-2643- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.
CVE-2015-2643: Fixed in MariaDB 10.0.20
- CVE-2015-2620- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Security : Privileges.
CVE-2015-2620: Fixed in MariaDB 10.0.20
- CVE-2015-2582- Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to GIS.
CVE-2015-2582: Fixed in MariaDB 10.0.20
- CVE-2015-2573- Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.
CVE-2015-2573: Fixed in MariaDB 10.0.17
- CVE-2015-2568- Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote attackers to affect availability via unknown vectors related to Server : Security : Privileges.
CVE-2015-2568: Fixed in MariaDB 10.0.17
- CVE-2015-0441- Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Encryption.
CVE-2015-0441: Fixed in MariaDB 10.0.17
- CVE-2015-0433- Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via vectors related to InnoDB : DML.
CVE-2015-0433: Fixed in MariaDB 10.0.17
- CVE-2015-2571- Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.
CVE-2015-2571: Fixed in MariaDB 10.0.18

- CVE-2015-0505- Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.
CVE-2015-0505: Fixed in MariaDB 10.0.18
- CVE-2015-0501- Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Compiling.
CVE-2015-0501: Fixed in MariaDB 10.0.18
- CVE-2015-0499- Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Federated.
CVE-2015-0499: Fixed in MariaDB 10.0.18
- CVE-2015-0432- Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier allows remote authenticated users to affect availability via vectors related to Server : InnoDB : DDL : Foreign Key.
CVE-2015-0432: Fixed in MariaDB 10.0.16
- CVE-2015-0411- Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier, and 5.6.21 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Server : Security : Encryption.
CVE-2015-0411: Fixed in MariaDB 10.0.16
- CVE-2015-0382- Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote attackers to affect availability via unknown vectors related to Server : Replication, a different vulnerability than CVE-2015-0381.
CVE-2015-0382: Fixed in MariaDB 10.0.16
- CVE-2015-0381- Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote attackers to affect availability via unknown vectors related to Server : Replication, a different vulnerability than CVE-2015-0382.
CVE-2015-0381: Fixed in MariaDB 10.0.16
- CVE-2015-0374- Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Security : Privileges : Foreign Key.
CVE-2015-0374: Fixed in MariaDB 10.0.16
- CVE-2015-0391- Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.
CVE-2015-0391: Fixed in MariaDB 10.0.13

Previous release notes can be found [here](#).

McAfee Technical Support

PrimeSupport ServicePortal: <https://mysupport.nai.com/login.asp>

Multi-National Phone Support: <http://www.mcafeesecurity.com/us/contact/home.htm>

This message may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2011-2016 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates.