CVE-2016-6662 MySQL

This article was last updated on: Oct 27, 2017 15:04

IN PROGRESS This article is still under investigation and will be updated as new information is available. Check back often for the most current information.

Background Information

On 12 September, 2016, an independent researcher revealed multiple MySQL vulnerabilities. This advisory focuses on a vulnerability with a CVEID of CVE-2016-6662 which can allow attackers to (remotely) inject malicious settings into MySQL configuration files (my.cnf) under certain configurations, leading to critical consequences.

More information on MySQL can be found on the following websites:

http://www.mysql.com/products/

http://www.mysql.com/why-mysql/

http://db-engines.com/en/system/MySQL

MySQL derivatives are also affected, including:

MariaDB - https://mariadb.org/
PerconaDB - https://www.percona.com/software/mysql-database/percona-server

---

Impact

The vulnerability affects all MySQL servers in the default configuration in all version branches (5.7, 5.6, and 5.5) including the latest versions, and can be exploited by both local and remote attackers. Both the authenticated access to MySQL databases (via network connection or web interfaces such as phpMyAdmin) and SQL Injection could be used as exploitation vectors if a MySQL user has the ***SUPER*** privilege granted. Additionally, MySQL users with both ***SELECT*** and ***FILE*** privileges granted are also affected.

MySQL users created in cPanel are **not** granted the ***SUPER*** or ***FILE*** privileges, however they can be granted these elevated privileges from the root MySQL user manually.

A successful exploitation could allow attackers to execute arbitrary code with root privileges which would then allow them to fully compromise the server on which an affected version of MySQL or MariaDB is running.

How to determine if your server is affected

Determine if you are running MySQL or MariaDB

You can determine if MySQL is installed by running the following command as root:

```
# yum list installed | grep MySQL | grep -server
MySQL56-server.x86_64                          5.6.31-2.cp1156
installed
```

If you have confirmed you are running MySQL continue to the MySQL section below.

If the above command does not return any output, verify you are running MariaDB by running the following command as root:

```
# yum list installed | grep MariaDB | grep -server
MariaDB-server.x86_64                          10.0.27-1.el7.centos
@MariaDB100
```

If you have confirmed you are running MariaDB, continue to the MariaDB section below.

MySQL

cPanel is currently working on new versions with updated MySQL RPMs. We will update this section once new versions are available.

MariaDB

MariaDB has fixes in place for versions greater than 10.0.27 and 10.1.17. Run the following command as root to check the MariaDB version:

```
# rpm -q MariaDB-server
MariaDB-server-10.0.26-1.el7.centos.x86_64
```

If the MariaDB version is not greater than 10.0.27 or 10.1.17, see the resolution section below under MariaDB to update.

Resolution

MySQL

The following table lists the MySQL versions with updated RPMs and their corresponding cPanel & WHM versions:

MySQL version	cPanel & WHM version	Documentation
5.6.32	58.0.30	https://dev.mysql.com/doc/relnotes/mysql/5.6/en/news-5-6-33.html
5.5.52	58.0.30	https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-52.html

MariaDB

Versions 10.0.27 and greater are protected for 10.0.x versions of MariaDB, while versions 10.1.17 are protected for 10.1.x versions of MariaDB. If you are running an older version of MariaDB, you can upgrade with the following command:

```
# yum update MariaDB-server MariaDB-client MariaDB-common MariaDB-devel
MariaDB-shared
```

Mitigation

Warnings

- Manual modifications to the MySQL configuration always carries risk; a qualified systems administrator is recommended.
- We **strongly** recommend that you backup your databases before performing any of the steps below.

In most situations, these mitigations are not necessary as unprivileged MySQL users created in cPanel & WHM do not have the SUPER or FILE grants.

You can check if you have MySQL accounts, other than root, with these privileges granted manually by running the following commands as root:

```
# mysql mysql -e 'select User,Host from user where User != "root" and (
File_priv = "Y" or Super_priv = "Y" );'
#
```

If waiting for new cPanel versions with updated MySQL RPMs or upgrading to MariaDB is not possible, consider mitigating this issue by running the following commands as root:

```
# chown root:root /etc/my.cnf
# chmod 0644 /etc/my.cnf
```

This will ensure /etc/my.cnf is not writable by the MySQL user.

Additionally, you can touch empty root-owned files at /var/lib/mysql/my.cnf and /var/lib/mysql/.my.cnf to prevent MySQL users with SUPER or FILE privileges from potentially writing to other configuration paths that may be used on certain OS and MySQL version combinations. This may cause warnings to be logged when restarting MySQL.

```
# touch /var/lib/mysql/my.cnf /var/lib/mysql/.my.cnf
```

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- CVE-2016-6662 MySQL
- How to Configure MySQL SSL Connections
- How to Delete a MySQL Database

- How to Replace MySQL with Percona
- How to Restore a User's Database Access

- MySQL Database Wizard
- Remote MySQL
- MySQL Databases

- CVE-2016-6662 MySQL
- How to Configure MySQL SSL Connections
- How to Delete a MySQL Database
- How to Replace MySQL with Percona
- How to Restore a User's Database Access

- WHM API 1 Functions - set_postgresql_password
- WHM API 1 Functions - remote_mysql_validate_profile
- WHM API 1 Functions - rename_mysql_database
- WHM API 1 Functions - start_background_mysql_upgrade
- WHM API 1 Functions - remote_mysql_read_profile