# BOLETÍN DE ALERTA

**Boletín Nro.**: 2016-12
**Fecha de publicación**: 13/09/2016
**Tema**: Vulnerabilidades críticas en MySQL y sus ramas

**Sistemas afectados:**

- MySQL 5.7.15 y todas las versiones previas de dicha rama
- MySQL 5.6.33 y todas las versiones previas de dicha rama
- MySQL 5.5.52 y todas las versiones previas de dicha rama

Forks de MySQL:

- MariaDB
- PerconaDB

**Descripción**:

Recientemente se han descubierto y revelado múltiples vulnerabilidades críticas en MySQL, uno de los sistema de gestión de base de datos de código abierto más utilizados. La vulnerabilidad más crítica, identificada como CVE-2016-6662, afecta a los servidores MySQL en todas las ramas de la versión (5.7, 5.6, y 5.5) incluidas las últimas versiones, y podría ser explotada tanto de forma local como remota.
Tanto el acceso autenticado a la base de datos MySQL (a través de conexiones de red o interfaces web como phpMyAdmin) y la inyección de SQL podría utilizarse como vectores de explotación. Teniendo en cuenta que los ataques de inyección SQL son uno de los problemas más frecuentes en las aplicaciones web, esta vulnerabilidad pone en riesgo a numerosas aplicaciones web. Una vez con acceso a la base de datos, se podría inyectar líneas de código maliciosas en los ficheros de configuración my.cnf.

Debido a que todas las versiones de MySQL usan el script mysqld_safe como un wrapper para iniciar el servicio de MySQL que se ejecuta como root, y teniendo en cuenta que este script puede utilizarse para precargar una librería compartida antes de iniciar el servidor, esta librería podría ser especificada



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

con el parámetro --malloc-lib=LIB o directamente en la sección '[mysqld]' o '[mysqld_safe]' del fichero de configuración my.cnf.
Si un atacante consigue inyectar una línea en ese fichero de configuración podría ser capaz de cargar una librería maliciosa y ejecutar código como root en el momento en que se reinicie el servicio de MySQL. Existen diversas maneras a través de la cual un atacante podría realizar dicha inyección:

1. Inyectando configuraciones maliciosas en ficheros de configuración de MySQL existentes con permisos débiles. Esto es que es un error que los ficheros de configuración pertenezcan y sean escribibles por el usuario mysql.
2. Creando nuevos ficheros de configuración en el directorio data de MySQL (escribible por defecto por el usuario mysql), concretamente en /var/lib/mysql/. Existe otra vulnerabilidad con un CVEID de CVE-2016-6663 pendiente de la divulgación que supuestamente hará que sea más fácil crear /var/lib/mysql/my.cnf sin el requisito del permiso FILE.
3. Los atacantes con permisos sólo de SELECT/FILE pueden conseguir acceso a funciones de logging (normalmente sólo disponibles para usuarios administradores de MySQL) en todas las instalaciones por defecto para poder añadir/modificar ficheros de configuración.

Oracle todavía no ha disponibilizado parches oficiales para la vulnerabilidad para Oracle MySQL Server. La vulnerabilidad puede ser explotada incluso si los módulos de seguridad SELinux y AppArmor se encuentran instaladas, con políticas activas por defecto, en las principales distribuciones de Linux. El investigador que ha descubierto las vulnerabilidades ha publicado una prueba de concepto (limitada) de la explotación de dichas vulnerabilidades, debido a la falta de respuesta del fabricante. Así mismo, otras pruebas de concepto más detalladas han empezado a publicarse. Otros gestores de bases de datos afectados, como MariaDB o PerconaDB, aplicaron los parches correspondientes el pasado 30 de agosto.

**Impacto**:
Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario con privilegios de root, obteniendo así un control total sobre el servidor en el cual se está ejecutando una versión vulnerable de MySQL.

**Mitigación:**



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

Como mitigación temporal, se recomienda que los administradores se aseguren de que ningún usuario de la base de datos sea propietario de ningún fichero de configuración MySQL, así como también generar ficheros "trampa" *my.cnf* de root que no sean utilizados para el funcionamiento normal de la base de datos.
Sin embargo se debe recordar que estos son de ninguna manera una solución completa y los usuarios deben aplicar los parches oficiales de proveedores tan pronto como estén disponibles.

**Información adicional:**
http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html
http://www.hackplayers.com/2016/09/0-day-en-mysql-permite-ejecucion-remota.html
http://seclists.org/oss-sec/2016/q3/484



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py