

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE (S) ISSUED:**

6/12/2012

**SUBJECT:**

Vulnerability in MySQL Could Allow Authentication Bypass

**OVERVIEW:**

A security bypass vulnerability has been discovered in multiple versions of MySQL that could allow attackers to take complete control of affected databases. MySQL is a relational database management system that is used to correlate and organize data.

Successful exploitation could result in an attacker gaining access to the database. Depending on the privileges associated with the user, an attacker could then insert, view, change, or delete data in the database; or create new database accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**It should be noted that official builds from MySQL and MariaDB (including Windows) as well as SuSE 9.3, Debian and systems using official RHEL rpms are not affected by this vulnerability.**

**SYSTEMS AFFECTED:**

MySQL versions up to 5.1.61, 5.2.11, 5.3.5, 5.5.22 running on Debian Unstable, Ubuntu, Fedora and Open SuSE operating systems

**RISK:**

**Government:**

Large and medium government entities: **High**

Small government entities: **High**

**Businesses:**

Large and medium business entities: **High**

Small business entities: **High**

**Home users: N/A**

**DESCRIPTION:**

MySQL is prone to an authentication bypass vulnerability that could allow unauthorized users access a MySQL database. This vulnerability is caused when the Linux glibc library is compiled using an unsafe optimized version of the C function "memcmp". To exploit this vulnerability an attacker must be able to access the MySQL database, whether it be local or remote (if allowed). The attacker can then attempt to brute force the MySQL passphrase if a username is known. After a number of failed brute force attempts MySQL's authentication controls will be overridden allowing any password to be accepted causing the authentication bypass.

Successful exploitation of this vulnerability could allow an attacker gaining the same privileges as a database user account. Depending on the privileges associated with the user, an attacker could then insert, view, change, or delete data in the database; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

Official vendor MySQL and MariaDB binaries are currently not known to be vulnerable to this vulnerability.

**It should be noted that official builds from MySQL and MariaDB (including Windows) as well as SuSE 9.3, Debian and systems using official RHEL rpms are not affected by this vulnerability.**

**RECOMMENDATIONS:**

The following actions should be taken:

- Update MySQL to versions 5.1.63, 5.5.24, or 5.6.6

- Do not allow access to the MySQL database from the Internet, if there is no documented business need, by blocking port 3306 (MySQL) at the perimeter firewall.

- MySQL configuration files should be checked to ensure that access to the database is restricted to authorized hosts.

**REFERENCES:**

**Rapid7:**

<https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql>

**Oracle:**

<http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html>

**Ubuntu:**

<http://www.ubuntu.com/usn/usn-1467-1/>

**Securityfocus:**

<http://www.securityfocus.com/advisories/25113>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122>