NTT DATA
NTTデータ 先端技術株式会社

MySQL の memcmp 関数処理における不備により認証を回避される脆弱性 (CVE-2012-2122)に関する検証レポート

2012/6/15
NTT データ先端技術株式会社
辻　伸弘
川島　祐樹
小松　徹也

【概要】

MySQL サーバに、ログイン認証を回避される脆弱性が存在します。
この脆弱性は、認証時に利用される SSE 最適化された memcmp 関数の返り値のチェックに問題があり、認証を回避されます。

この脆弱性により、攻撃者が認証情報を複数回送信し、特定条件における認証を回避することで、任意のユーザ権限でデータベースを操作される危険性があります。また、認証試行は、1/256 程度の確率で回避することが可能です。今回、この MySQL サーバの認証を回避される脆弱性（CVE-2012-2122）の再現性について検証を行いました。

【影響を受けるとされているシステム】

- Ubuntu Linux 64-bit (10.04, 10.10, 11.04, 11.10, 12.04) (via many including @michealc)
- OpenSuSE 12.1 64-bit MySQL 5.5.23-log (via @michealc)
- Debian Unstable 64-bit 5.5.23-2 (via @derickr)
- Fedora (via hexed and confirmed by Red Hat)
- Arch Linux (unspecified version)

※上記の情報は、PoC コードおよび実証ベースの検証情報を共有するサイトより引用

2012 年 6 月 15 日現在、影響を受けるシステムの範囲や条件が公式に掲載されておりません。そのため、本レポートでは、検証情報を提供するサイトより情報の引用をしています。これらの情報は、あくまでも暫定的なものですので、ご使用のシステムに関してはそれらを提供するベンダーへ影響について確認していただくことを推奨いたします。

脆弱性に該当する明確な条件の情報公開までの間に管理するサーバの確認する必要がある場合は、以下のコードで確認できます。

> このコードは自身の管理下にないネットワーク・コンピュータに行った場合は、攻撃行為と判断される場合があり、最悪の場合、法的措置を取られる可能性もあります。このコードを利用する場合は、くれぐれも許可を取ったうえで、自身の管理下にあるネットワークやサーバに対してのみ行ってください。以下のコードを利用することで発生した問題に関しましては、弊社は一切の責任を負いかねますことをご了承ください。

```
for i in `seq 1 1000`; do mysql -u root --password=bad -h 127.0.0.1 2>/dev/null; done
```

ローカルからの調査を前提としていますが、対象ホスト指定を変更することで、リモート環境についても確認できます。成功するまでは、ログイン処理を実施するため、稼働中のサーバへ影響を考慮してください。

Windows および Red Hat Enterprise Linux4、5 および 6 は、影響をうけないことが確認されています。

【対策案】

ベンダーよりこの脆弱性の修正プログラムがリリースされております。
当該脆弱性が修正されたプログラムを適用していただくことを推奨いたします。

MySQL.com: MySQL Server Changelog
http://dev.mysql.com/doc/refman/5.5/en/news-5-5-24.html
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-63.html

※パッケージ管理された MySQL を利用している場合は、各々のベンダーの提供するパッチ情報を参照の上、適用していただくことを推奨いたします。

パッケージを提供する各々のベンダにてパッチが提供されていない、または、なんらかの理由から対策を講じることができない場合、ファイアウォールやネットワーク機器を用いて、適切なホストからのアクセスのみを許可するといった通信上の制御を行っていただくことを推奨いたします。

また、MySQL の設定ファイル（通常は、my.cnf）を用いて待ち受けに使用するアドレスを指定可能です。ローカルによるアクセスのみの運用を行っている場合は以下のように記述することで外部からの接続を受け付けないようにすることが可能です。

```
bind-address = 127.0.0.1
```

【参考サイト】

OSVDB: MySQL Authentication Protocol Token Comparison Casting Failure Password Bypass
http://www.osvdb.org/show/osvdb/82804

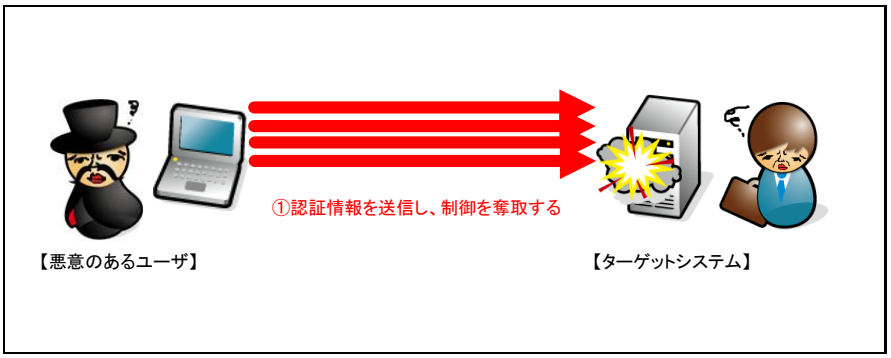
RedHat: incorrect type cast in check_scramble() leading to authentication bypass
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-2122
https://access.redhat.com/security/cve/CVE-2012-2122

Ubuntu: Ubuntu Security Notice USN-1467-1
http://www.ubuntu.com/usn/usn-1467-1/

Novell: CVE-2012-2122: mysql: authentication bypass due to incorrect type casting
https://bugzilla.novell.com/show_bug.cgi?id=765092
http://support.novell.com/security/cve/CVE-2012-2122.html

Debian: CVE-2012-2122
http://security-tracker.debian.org/tracker/CVE-2012-2122

【検証イメージ】



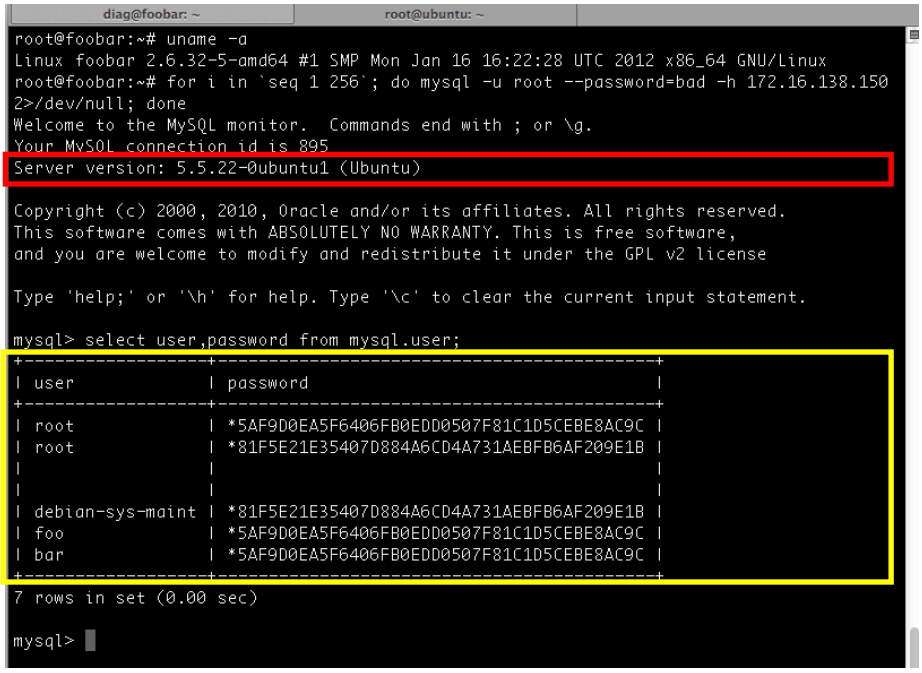
【検証ターゲットシステム】
Ubuntu 12.04 LTS 上の MySQL Server 5.5.22-0ubuntu1

【検証概要】
ターゲットシステムに、複数の認証情報を送信し、特定条件において認証を回避してログインします。
今回の検証に用いたコードは、ターゲットシステム上の MySQL サーバに接続し、MySQL サーバの制御を奪取するものです。
これにより、リモートからターゲットシステム上の MySQL サーバが操作可能となります。
** 対象ターゲットのシステムは Ubuntu 12.04 LTS です。*

【検証結果】
下図の赤線で囲まれている部分の示すように、ターゲットシステム上の MySQL サーバにログイン画面が表示されています。
黄線で囲まれている部分の示すように、ターゲットシステム上の MySQL サーバのパスワード情報を取得した結果が表示されています。これにより、MySQL Serve のパスワード情報の奪取に成功したと言えます。

NTT DATA
NTTデータ 先端技術株式会社

MySQL サーバのパスワード情報奪取に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部　営業担当　サービス企画戦略グループ
TEL：03-5859-5422
http://security.intellilink.co.jp