

phpMyAdmin の setup.php の脆弱性(CVE-2009-1151)に関する検証レポート

2009/6/12
 診断ビジネス部
 辻 伸弘
 松田 和之

【概要】

phpMyAdmin の setup.php ファイルに脆弱性が存在することが発見されました。この脆弱性により、リモートから Web サービスの実行権限で任意のコマンドが実行可能となります。

想定される被害としては、悪意のあるユーザにより、Web サービスの実行権限での情報取得、改ざん、または、悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、この脆弱性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】

phpMyAdmin 2.11.9.5 より前のバージョン

phpMyAdmin 3.1.3.1 より前のバージョン

上記のバージョンの phpMyAdmin を利用していて、かつ、セットアップ時に以下の手順を実施した後、config ディレクトリを削除していない場合に影響を受けます。

「http://www.phpmyadmin.net/documentation/#setup_script」より抜粋

```
cd phpMyAdmin
mkdir config
chmod o+rw config
cp config.inc.php config/
chmod o+w config/config.inc.php
```

【対策案】

最新バージョン (phpMyAdmin 2.11.9.5、または、phpMyAdmin 3.1.3.1) へアップデートすることが推奨されます。
http://www.phpmyadmin.net/home_page/downloads.php

また、phpMyAdmin のセットアップ時に利用したファイル「config/config.inc.php」の有無を確認し、存在する場合、削除することが暫定的な対策となります。

なお、セットアップファイル「config/config.inc.php」はデフォルトでは存在しません。

【参考サイト】

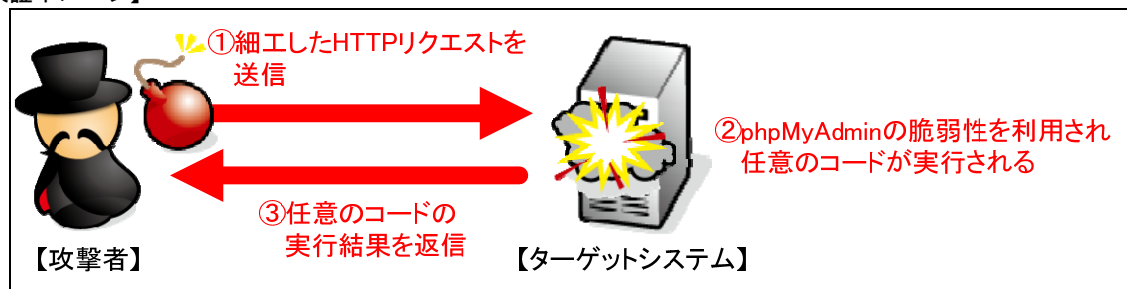
CVE-2009-1151

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1151>

phpMyAdmin - Security - PMASA-2009-3

http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

【検証イメージ】



【検証ターゲットシステム】

phpMyAdmin 3.0.1.1
phpMyAdmin 2.11.9.4

【検証概要】

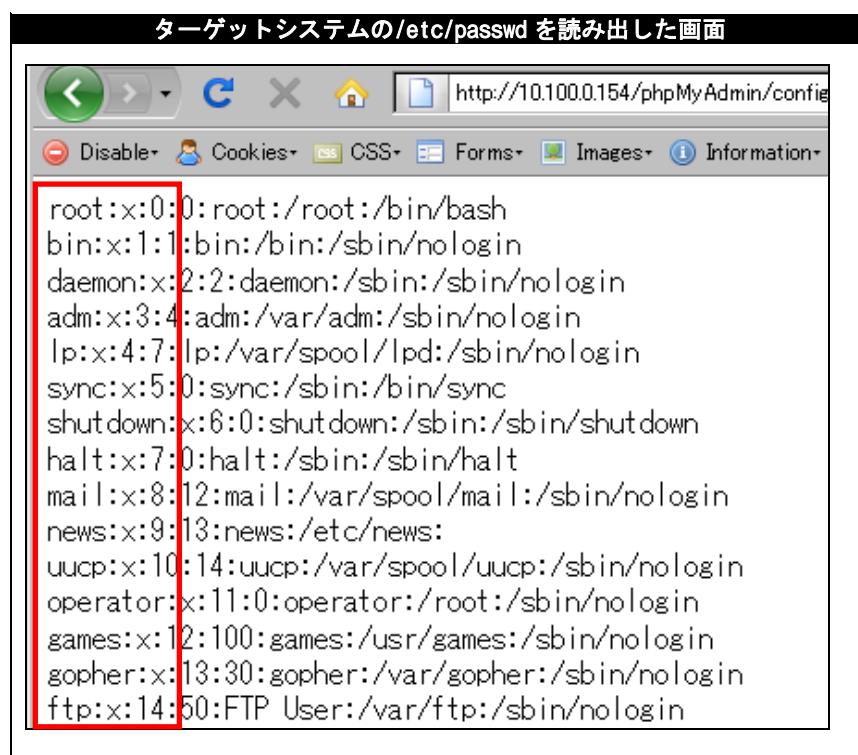
ターゲットシステムに、細工した HTTP リクエストを送信することで、任意のコマンドを実行します。

【検証結果】

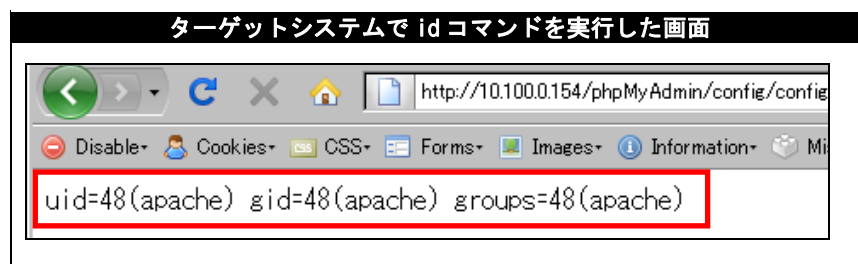
下図は、phpMyAdmin の setup.php の脆弱性を利用し、ターゲットシステムのユーザ情報が格納されている「/etc/passwd」ファイルを、ブラウザから読み出した画面です。

赤枠（赤枠内の「:」(コロン) より前の部分) で示すとおり、ターゲットシステムに存在するユーザの一覧の取得に成功したと判断できます。これにより、悪意のあるユーザに、SSH 等から当該ユーザに対するオンラインクラックを行われ、システムへの更なる制御の奪取を許す危険性があります。

また、プログラムのソースコードも閲覧可能であるため、ソースコードにパスワードが書かれている場合、パスワードを取得され、なりすましに利用される危険性があります。



下図は、ターゲットシステム上で id コマンドを実行した画面です。このことから、当脆弱性を利用することで、Web サービスの実行権限でのコマンド実行が可能であると判断できます。つまり、Web サービスが管理者権限で稼働している場合、ターゲットシステムに存在する暗号化されたパスワードも読み出すことが可能となります。





NTTデータ・セキュリティ株式会社

【対策案】

最新バージョン（phpMyAdmin 2.11.9.5、または、phpMyAdmin 3.1.3.1）へアップデートすることが推奨されます。
http://www.phpmyadmin.net/home_page/downloads.php

また、phpMyAdmin のセットアップ時に利用したファイル「config/config.inc.php」の有無を確認し、存在する場合、削除することが暫定的な対策となります。

なお、セットアップファイル「config/config.inc.php」はデフォルトでは存在しません。

【参考サイト】

CVE-2009-1151

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1151>

phpMyAdmin - Security - PMASA-2009-3

http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

*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・セキュリティ株式会社

営業企画部

TEL:03-5425-1954

<http://www.nttdata-sec.co.jp/>