NTTデータ・セキュリティ株式会社

WordPress の file.php の脆弱性に関する検証レポート

2009/11/18
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

オープンソースのブログソフトウェアである「WordPress」の file.php（ファイルアップロード用プログラム）に任意の実行ファイルがアップロード可能な脆弱性が存在することが発見されました。

WordPress は、ひとつのブログを複数のユーザで管理することが想定されており、管理者が各ユーザに利用できる機能を制限できるように設計されています。
さらに、実行ファイルのアップロードについてはセキュリティ上制限されており、アップロードできない設計となっています。

しかし、今回の脆弱性を利用されることにより、アップロードのセキュリティ制限を回避され、悪意ある投稿権限を持つユーザに、バックドア用の実行ファイルをアップロードされ、外部から Web サービスの実行ユーザ権限で任意のコマンドを実行される危険性があります。

今回、この WordPress の file.php 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】

WordPress 2.8.5 以下のバージョン

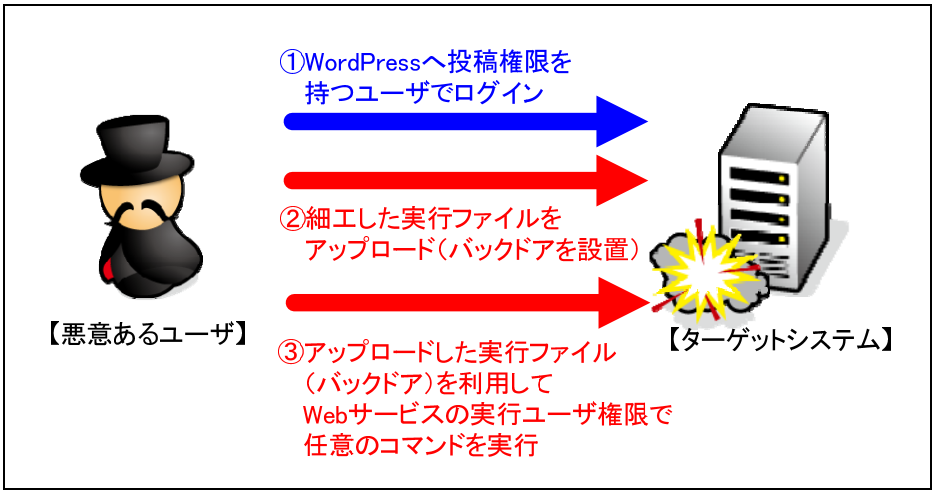
【対策案】

最新バージョン（WordPress 2.8.6）へアップデートすることが推奨されます。
http://wordpress.org/download/

【参考サイト】

WordPress 2.8.6 Security Release
http://wordpress.org/development/2009/11/wordpress-2-8-6-security-release/

【検証イメージ】



NTTデータ・セキュリティ株式会社

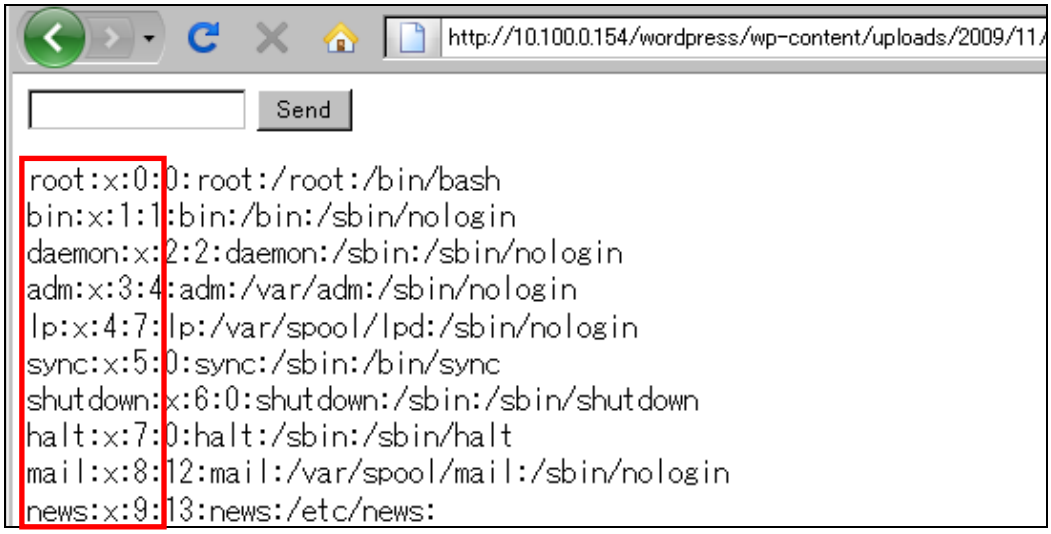
【検証ターゲットシステム】
Aapche 2.2.3 (httpd-2.2.3-22.el5.centos.1)
WordPress 2.8.5

【検証概要】
WordPress に投稿権限を持つユーザでログインし、細工した実行ファイルをアップロード（バックドアを設置）することで、ブラウザから Web サービスの実行ユーザ権限での任意のコマンド実行を試みます。

※本脆弱性は、WordPress にファイルアップロード権限を持つユーザでログインできることが前提条件です。ログインしない状態で攻撃の影響を受けることはありません。

【検証結果】
下図は、バックドア設置後、バックドアを利用して、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。

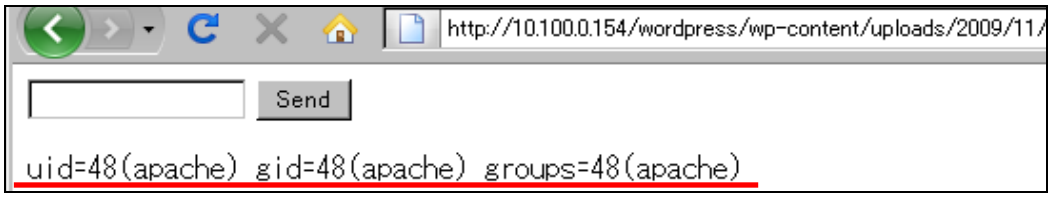
ターゲットシステムの/etc/passwd を読み出した画面



NTTデータ・セキュリティ株式会社

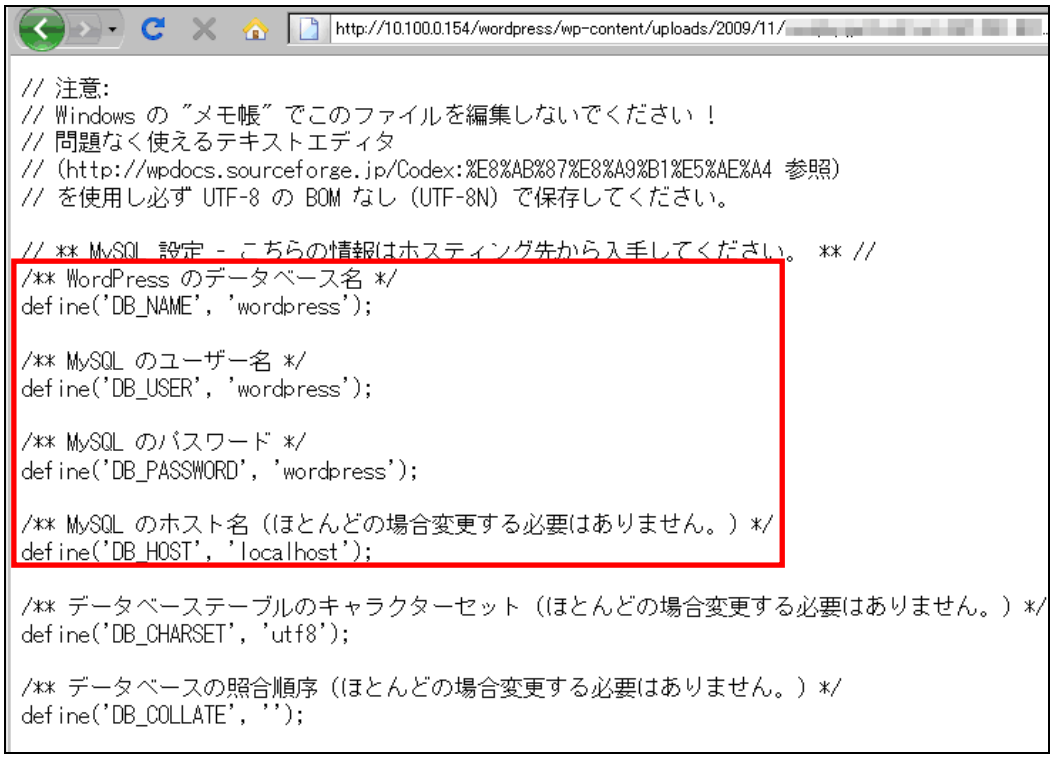
下図は、ターゲットシステム上で id コマンドを実行した画面です。このことから、当脆弱性を利用することで、Web サービスの実行ユーザ権限でのコマンド実行が可能であると判断できます。つまり、Web サービスが管理者権限で稼動している場合、ターゲットシステムに存在する暗号化されたパスワードも読み出すことが可能となります。

ターゲットシステムで id コマンドを実行した画面



下図は、WordPress の設定ファイル（wp-config.php）を、ブラウザから読み出した画面です。
赤枠で示すとおり、WordPress が利用するデータベース情報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、データベースへ侵入され、データの閲覧、改ざん、削除を行われ、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。

ターゲットシステムの WordPress の設定ファイルを読み出した画面



＊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・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/