SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

WordPress のクロスサイトスクリプティングの脆弱性に関する(CVE-2015-3440)調査レポート

【概要】

CMS(*1)ソフトウェアとして広く使われている WordPress に クロスサイトスクリプティングの脆弱性(CVE-2015-3440)が発見されました。この脆弱性は、WordPress に、コメントの大量の文字列の処理に不具合があるため、任意のスクリプトの挿入が可能です。

攻撃者は細工された文字列を WordPress の記事へのコメントを入力し送信することにより、任意のスクリプトをページ内に挿入し、コメントを表示したユーザーのブラウザ上で実行させることが可能です。これによりユーザーを悪意のあるサイトへと誘導しマルウェアを感染させたり、ページの一部を改ざんするといった攻撃が可能となります。

また、この脆弱性を WordPress の管理者権限をもったユーザーに対して任意のスクリプトを実行させることにより、システムを操作することが可能であるという報告が確認されています。

*1CMS(Content Management System の略):ウェブサイトのページ作成において、技術的な知識がなくても容易にページを作成できるような仕組みを用意したシステム。

【影響を受ける可能性があるシステム】

- WordPress 4.2
- WordPress 4.1.2
- WordPress 4.1.1
- WordPress 3.9.3

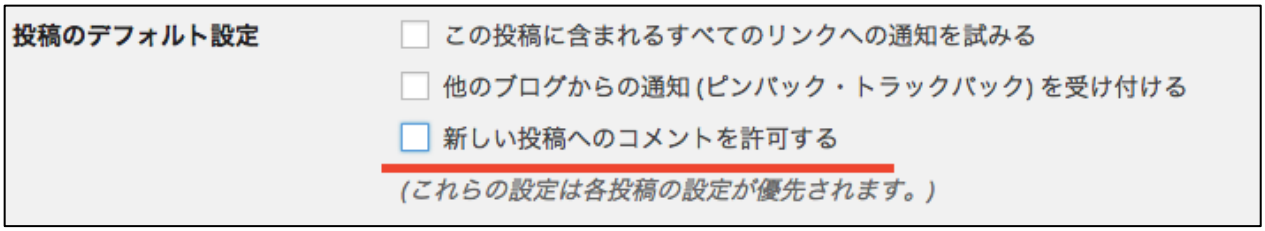
【対策案】

wordpress.org より、この脆弱性を修正するプログラムがリリースされています。当該脆弱性の修正を含む最新のバージョンを適用していただくことを推奨いたします。(2015/4/29 時点の最新バージョンは 4.2.1 です)

- Download WordPress

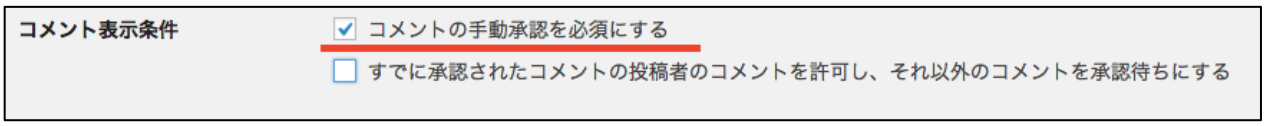
ただちに最新版へとアップデートすることが困難な場合、コメント機能を無効にしていただくか、コメントの承認機能を有効にし、承認なしでのコメントの掲載を制限することを推奨します。記事へのコメント機能の無効化、コメントの承認制機能の有効化は以下の方法を参考にしてください。

・ 記事へのコメント機能の無効化方法(WordPress 4.1.1 日本語版にて確認)
新規の投稿 :設定-ディスカッション [新しい投稿へのコメントを許可しない]のチェックを外して
[変更を保存]を押してください。



過去の投稿：投稿の編集画面から記事の編集を行い、コメントを[許可しない]に変更してください。
参考:[コメントを有効化・無効化する ‹ サポート ‹ WordPress.com]

・ コメントの承認機能の有効化（WordPress 4.1.1 日本語版にて確認）
設定−ディスカッション−[コメントの手動承認を必須にする]のチェックをいれて[変更を保存]を押してください。



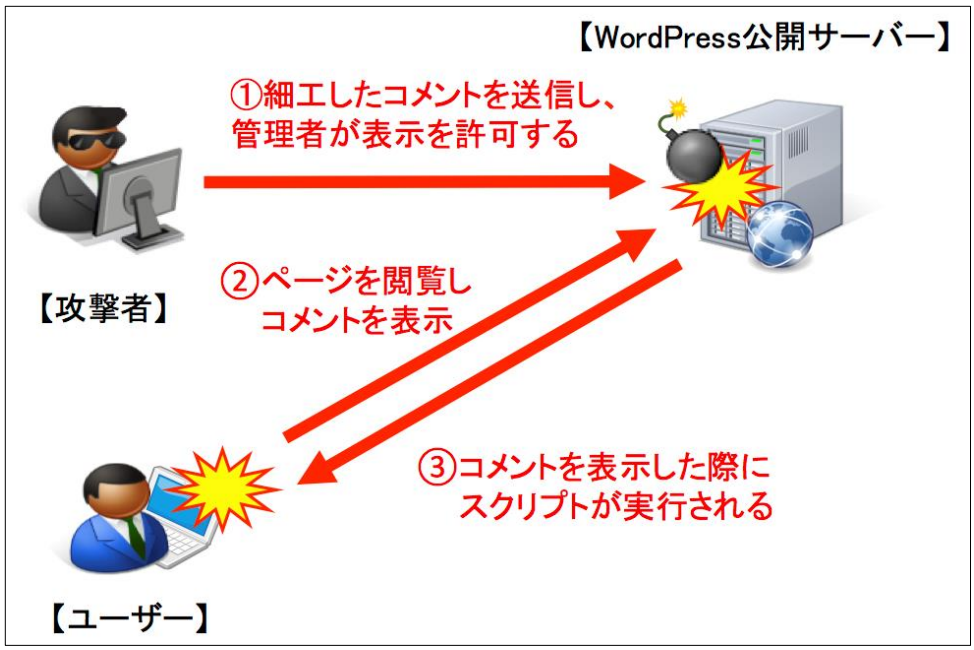
また、すぐ下の[すでに承認されたコメントの投稿者のコメントを許可し、それ以外のコメントを承認待ちにする]のチェックは外しておくことを推奨します。攻撃者が、一度無害なコメントを送信し、投稿者として許可を得た上で、２回目以降に悪意のあるコメントを送信する可能性があるためです。

【参考サイト】
− WordPress 4.2.1 Security Release
− CVE−2015−3440 (debian.org)

【検証概要】
WordPress のコメント欄に任意のメッセージダイアログを出すスクリプトを挿入し、コメントを反映した後、他のユーザーがページを開いた際にダイアログを表示されることを確認します。これにより、第三者がコメントを利用することにより、任意のスクリプトを挿入できることが確認できます。

【検証ターゲットシステム】
WordPress 4.1.2 日本語版 （Debian GNU/Linux）

【検証イメージ】

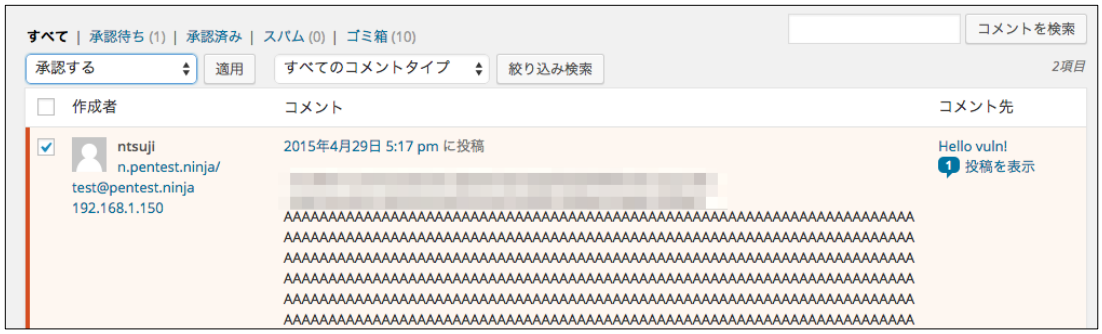


【検証結果】

攻撃者が任意のスクリプトをコメント欄に記入して[画像1]、投稿後、コメントの表示を管理者が許可し[画像2]、コメントの内容がページに挿入されました。

［画像1］

[画像2]



利用者がページを閲覧し、マウスカーソルをページ内に移動すると、攻撃者が意図した任意のダイアログ[hello vuln]を表示させること[画像3]ができました。

[画像3]

これにより、攻撃者は任意のスクリプトをページ内に挿入可能であることが確認できました。

【更新履歴】

2015 年 4 月 30 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00
電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/