2019 年 2 月 5 日

サービス＆セキュリティ株式会社 e-Gate センター

WordPress 向けプラグインの脆弱性を狙った攻撃について

1. 概要

コンテンツマネジメントシステム（CMS）の WordPress 向けに提供されているスパムコメント対策用プラグイン「spam-byebye」に脆弱性が存在していることが報告されました。この脆弱性が悪用されると、同プラグインの設定ページへアクセスできるユーザの Web ブラウザ上で任意のスクリプトが実行される可能性があります。

また、WordPress 向けのプラグインである「Portable phpMyAdmin」では、約 6 年前に発見された脆弱性を狙った攻撃が昨年 11 月より急増し現在も検出され続けております。当セキュリティオペレーションセンター（以下、e-Gate センター）においても、昨年に引き続き当脆弱性を狙った攻撃が多く検出されております。この 2 つの脆弱性を突いた攻撃の動向と対策についてご紹介いたします。

2. WordPress 向けのプラグイン spam-byebye の脆弱性（CVE-2018-16206）について

JVN（脆弱性情報のポータルサイト）によりますと、WordPress 向けに提供されているスパムコメント対策用プラグインである spam-byebye には Web ページを出力する際の処理が不適切なために、任意のスクリプトが埋め込まれてしまう反射型のクロスサイトスクリプティングの脆弱性（CVE-2018-16206）があることが 2019 年 1 月に報告されました。この脆弱性が悪用されると、セッションハイジャックによる情報漏洩やマルウェア感染などの恐れがあり対策が必要です。

なお、e-Gate センターにおいて当脆弱性を狙った攻撃は本稿作成時点では確認されておりません。

対象プラグイン使用の有無やバージョンを確認し、使用されている場合は後述の対策を実施してください。

（1）攻撃概要

【攻撃の流れ】（図 1 と対応）

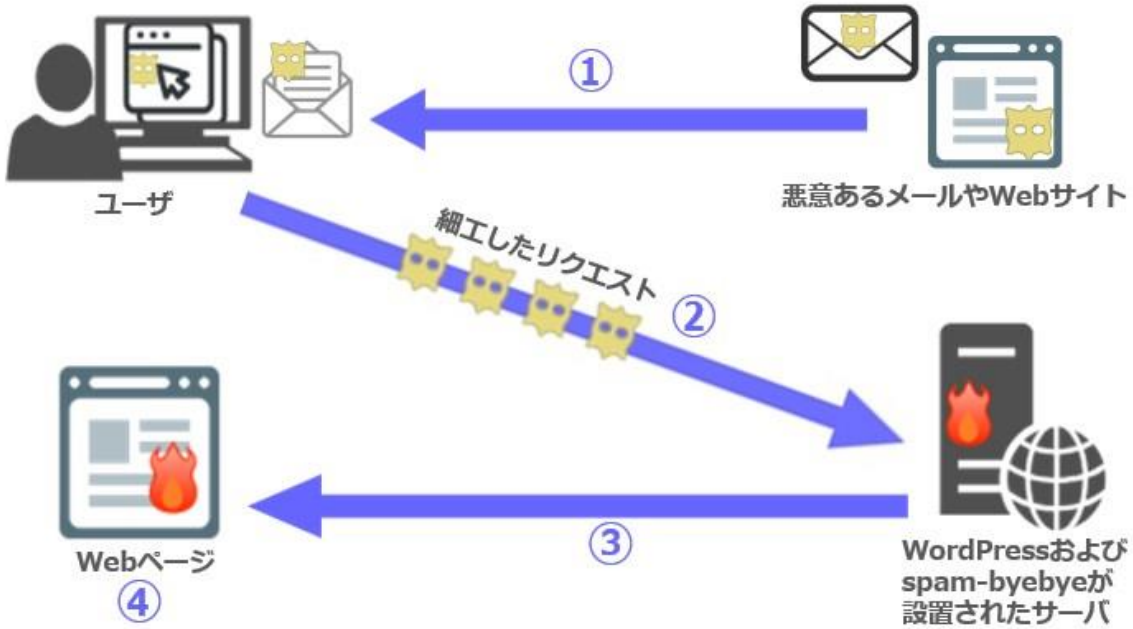
WordPress にログインしている状態のユーザが対象。

① Web サイトやメールに含まれる spam-byebye への悪意のあるリンクを表示する。

② 悪意のあるリンクを辿って spam-byebye にアクセスする際、細工されたリクエストが組み込まれる。

③ WordPress および spam-byebye が設置されたサーバにより、スクリプトを含むリクエストを元にページが作成される。

④ ページに含まれるスクリプトが実行される。



【図 1　spam-byebye の脆弱性を狙った攻撃イメージ】

（2）影響を受けるシステム

spam-byebye 2.2.1 およびそれ以前のバージョン

（3）想定される影響

spam-byebye のセットアップページにアクセスできるユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。

（4）対策

spam-byebye のバージョンを最新版へアップデートしてください。脆弱性を修正した spam-byebye 2.2.2 がリリースされております。

- WordPress spam-byebye プラグインのリリース情報
  https://wordpress.org/plugins/spam-byebye/

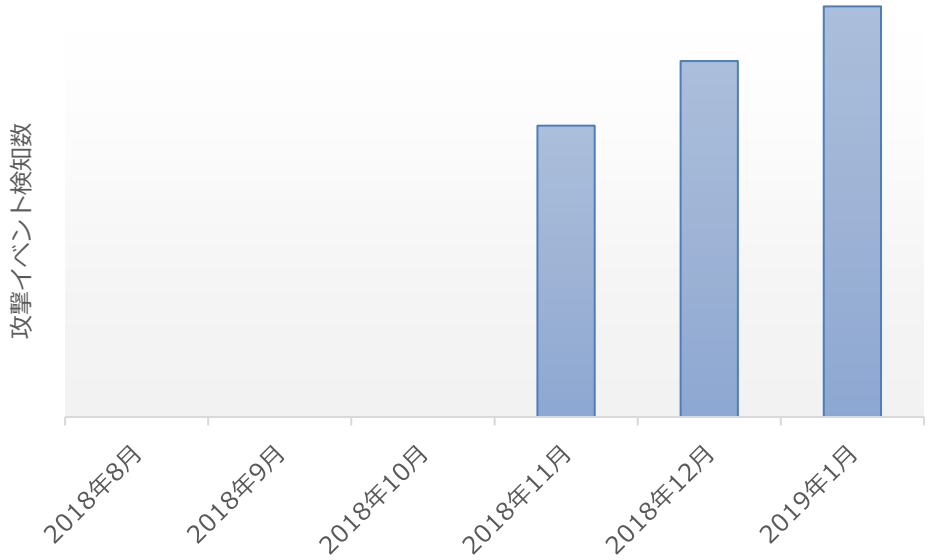
◆ 参考情報

- JVN iPedia 脆弱性対策情報データベース
  WordPress 用プラグイン spam-byebye におけるクロスサイトスクリプティングの脆弱性
  https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-000001.html

3. WordPress 向けプラグイン Portable phpMyAdmin の脆弱性（CVE-2012-5469）を狙った攻撃の増加

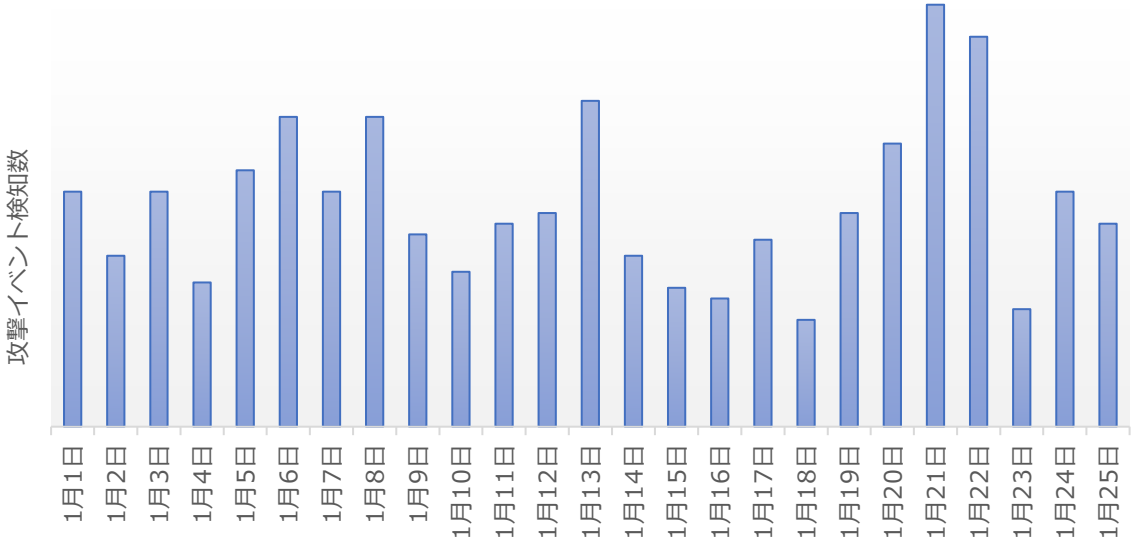
約 6 年前の WordPress 向けプラグイン Portable phpMyAdmin の脆弱性（CVE-2012-5469）を狙った攻撃が昨年 11 月から急増し、現在もなお観測され続けております。

e-Gate センターにおいても当脆弱性を狙った攻撃が多く検出されており、下記グラフは当攻撃イベントの検知数の推移を示しています。昨年 11 月から検出され始め、12 月、1 月と顕著に増加していることから、今後もさらに攻撃活動が活発となる可能性があり警戒が必要です。



【図 2　Portable phpMyAdmin の脆弱性を狙った攻撃イベント検知数の推移（直近 6 ヵ月）】

下記グラフは、当攻撃イベントの 2019 年 1 月（2019 年 1 月 25 日時点）の検知数の推移を示しております。連日、継続的に攻撃活動が観測されているため、しばらく注意が必要であると考えられます。



【図 3　Portable phpMyAdmin の脆弱性を狙った 2019 年 1 月の攻撃イベント検知数の推移】

（1）攻撃概要

Portable phpMyAdmin プラグインには認証を回避され、phpMyAdmin コンソールのアクセス権を取得される脆弱性が存在します。

（2）影響を受けるシステム

Portable phpMyAdmin 1.3.1 未満

（3）想定される影響

第三者により、wp-content/plugins/portable-phpmyadmin/wp-pma-mod への直接のリクエストを介して、phpMyAdmin に認証を回避してアクセスされる可能性があります。

（4）対策

下記 URL のベンダ情報および参考情報を参照して適切な対策を実施してください。

- WordPress　Portable phpMyAdmin プラグインのリリース情報
  https://wordpress.org/plugins/portable-phpmyadmin/#developers

◆ 参考情報

- JVN iPedia 脆弱性対策情報データベース
  WordPress　Portable phpMyAdmin プラグインにおける認証を回避される脆弱性
  https://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-005769.html

1. “e-Gate” の活用について

これらの脆弱性を狙ったサイバー攻撃を早期に発見する為には、日々のセキュリティ対策の運用監視が重要です。

また対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析・判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが肝要です。

24 時間 365 日体制のセキュリティ監視サービス “e-Gate“をご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、次世代 SOC “e-Gate センター“、この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルサポートするのが、SSK の “e-Gate” です。e-Gate センターを核として、人材・運用監視・対策支援という 3 つのサービスを軸に、全方位でのセキュリティサービスを展開しております。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp