2019 年 6 月 26 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：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（以下 CMS）は今や Web サイト構築には欠かせないものです。本年の 1 月に代表的な CMS である WordPress 向けのプラグインを狙った攻撃について紹介いたしましたが、5 月から 6 月にかけて新たに WordPress 用プラグインにおける脆弱性が相次いで報告されました。これらの脆弱性を悪用されることにより不正なアクセスや悪意のあるスクリプトを実行される可能性があります。本記事では、5 月から 6 月にかけて報告されたこれらの脆弱性を狙った攻撃の手法と動向・対策についてご紹介いたします。

2. 相次いで報告される CMS の脆弱性について

5 月から 6 月にかけて CMS 関連の脆弱性が報告されております。その中でも WordPress 用のプラグインを対象としたものが多数を占めています。これらの脆弱性を悪用されることにより、情報漏洩や Web ページの改ざん、マルウェア感染などの恐れがあり対策が必要です。

【5 月から 6 月にかけて JVN iPedia に公開された WordPress 用プラグインの脆弱性】

2019/06/24	JVNDB-2019-000042	プラグイン Custom CSS Pro の脆弱性
2019/06/24	JVNDB-2019-000041	プラグイン HTML5 Maps の脆弱性
2019/06/19	JVNDB-2019-000038	プラグイン Personalized WooCommerce Cart Page の脆弱性
2019/06/17	JVNDB-2019-000039	プラグイン Related YouTube Videos の脆弱性
2019/06/12	JVNDB-2019-000036	プラグイン Contest Gallery の脆弱性
2019/06/10	JVNDB-2019-000035	プラグイン Online Lesson Booking の脆弱性
2019/06/10	JVNDB-2019-000034	プラグイン Attendance Manager の脆弱性
2019/05/31	JVNDB-2019-000030	プラグイン Zoho SalesIQ の脆弱性
2019/05/23	JVNDB-2019-000028	プラグイン WP Open Graph の脆弱性

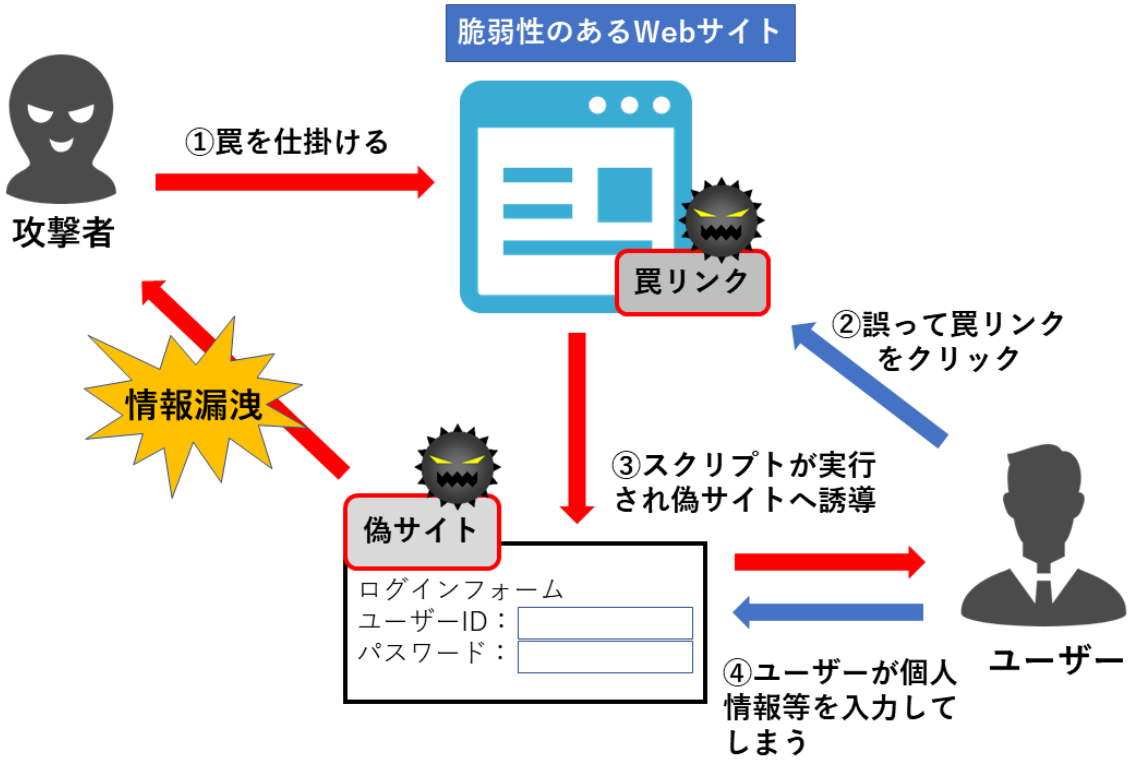
3. 攻撃の概要

前述で紹介しました WordPress 用のプラグインの脆弱性において、その対象となる攻撃手法は、いずれもクロスサイトスクリプティング（XSS）かクロスサイトリクエストフォージェリ（CSRF）です。これらの脆弱性を狙った代表的な攻撃手法であるクロスサイトスクリプティング（XSS）の概要と脅威について解説します。

クロスサイトスクリプティングは脆弱性のある Web サイトに悪意のあるスクリプトを埋め込み、そのスクリプトにユーザーが誘導されて重要な情報を盗まれたり、マルウェアに感染するという攻撃です。情報の入力や誘導される不正な URL リンクへのクリックなどに対し注意が必要ですが、これらのリンクが不正なものであるかを全て判断することは非常に困難です。

攻撃の流れは以下となります（下図１を参照）

① 攻撃者は脆弱性のある Web サイトを狙い、悪意のあるスクリプトを埋め込んだ罠リンクを用意します。
② ユーザーが誤って罠リンクをクリックすることで、悪意のあるスクリプトが実行されます。
③ 実行された悪意のあるスクリプトによりユーザーは、重要な個人情報などの入力を促す偽サイトなどに誘導されます。
④ ユーザーは偽サイトと気づかず、個人情報等を入力してしまいます。
これにより、重要情報の漏洩や、マルウェアに感染させるなどの被害が想定されます。

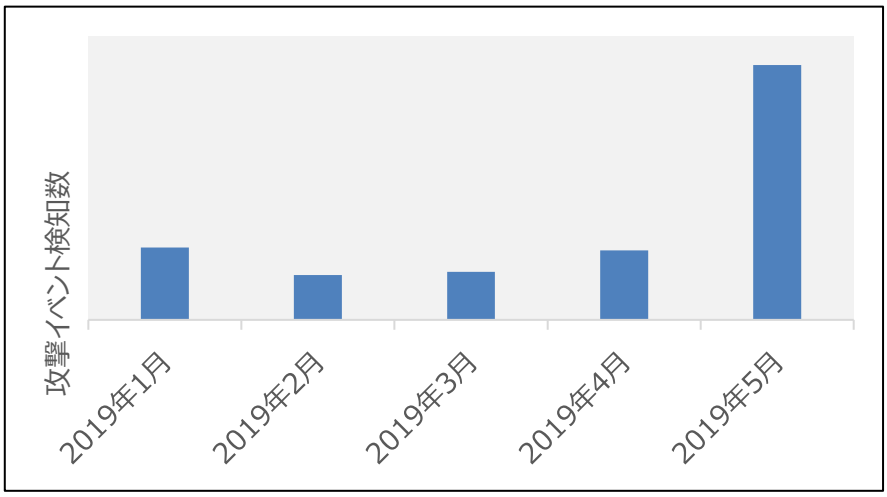


【図１ クロスサイトスクリプティング（XSS）の攻撃イメージ】

4. CMS の脆弱性を狙った攻撃の増加

このように Web サイトを狙った攻撃の足掛かりとなりやすいのが CMS の脆弱性ですが、当 e-Gate センターにおいても、CMS の脆弱性を狙った攻撃を多数観測しています。下記グラフは WordPress 以外にも、Joomla や Drupal 等の CMS の脆弱性を狙った攻撃イベントの検知件数の推移を示しています。

5 月になり攻撃イベント検知数が従来の 3 倍以上に急増しており、6 月現在も引き続き検知され続けています。これらの攻撃に警戒が必要です。



【図 2　e-Gate センターにて検知した CMS の脆弱性を狙った攻撃の検知件数の推移】

5. 対策

このような被害の可能性のある脆弱性を放置しておくことは情報の漏洩やサービスの不正利用などにより多大な損害を受ける可能性がある為、早急に対処することが重要です。

① 定期的な CMS やプラグインのセキュリティ情報の確認

脆弱性のある古いバージョンの CMS は攻撃者がスキャニングをおこなうことで、容易に特定することが可能です。当 e-Gate センターでもこれらのスキャニング通信を多数観測しています。これらの脆弱性に対しては、JVN の脆弱性情報や開発元ベンダのアップデート情報など信頼できるサイトのセキュリティ情報をもとに対処することが必要です。また、これらの情報は攻撃者にとっても攻撃の糸口となります。確認できた脆弱性に対してベンダ情報を参考にアップデートなどの適切な処置をいち早く行えるようにするため、定期的にセキュリティ情報をチェックすることを強く推奨いたします。

② セキュリティ機器・サービスの導入

セキュリティベンダの提供するセキュリティ機器やサービスを導入し適切に運用管理することにより、重要な情報の流出や被害の拡大を抑えることができます。

6. e-Gate の監視サービスについて

サイバー攻撃への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うことが重要です。“e-Gate“の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“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、最新のメソッド、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にサポートするのが 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のセキュリティサービスを展開しています。

【参考 URL】

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

7. 参考情報

■IPA セキュリティ情報

https://www.ipa.go.jp/security/announce/alert.html

■JVN iPedia

https://jvndb.jvn.jp/index.html

※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