2021 年 06 月 30 日

サービス＆セキュリティ株式会社 e-Gate センター

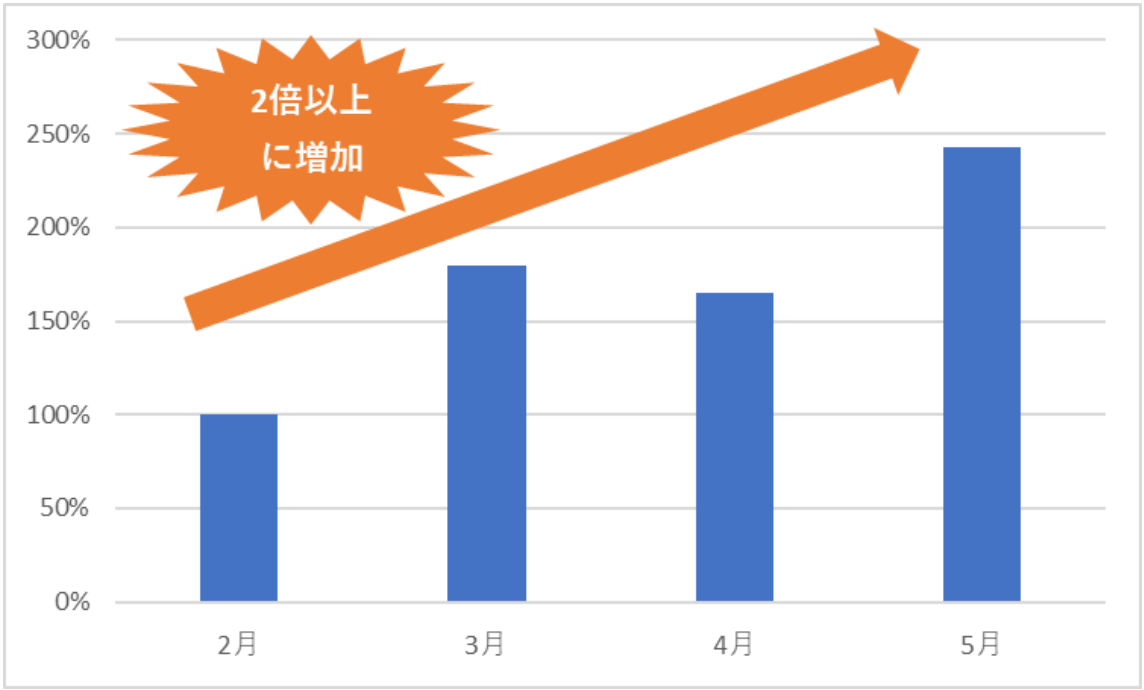
注意喚起：WordPress の脆弱性を突いた攻撃の増加について

1. 概要

WordPress はコンテンツマネジメントシステム（CMS）の 1 つです。日本国内での利用率 80%を超えており、Web サイトを作成するのに欠かせない存在となっています。一方で WordPress には多くの脆弱性が公表されており、脆弱性を突いた攻撃や種類は急増しているため利用の際は注意が必要です。今回は最近公表された脆弱性とその対策をご紹介いたします。

2. WordPress を狙った攻撃の増加

e-Gate センターでは WordPress を狙った攻撃通信が継続的に検知されています。以下は今年 2 月から今年 5 月までの 4 か月間の件数を表すグラフです。2 月と比べると 5 月の検知件数が 2 倍以上に増加しています。



【図 1】e-Gate センターにおける WordPress 関連の検知件数

攻撃方法に関しては過去に取り上げている以下の記事をご参照ください。

『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』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9892

3. 最近報告された WordPress の脆弱性

WordPress に関連する脆弱性は多数報告されています。5 月に JVN に掲載された WordPress 関連の脆弱性には以下のものがあります。4 月に公開されたのは 5 件でしたが、5 月には 12 件、6 月には 8 件と大きく増加しています。表 1 に 5 月から 6 月 28 日時点までの脆弱性情報を一覧化しました。20 件中色分けした 7 件がクロスサイトスクリプティングの脆弱性となっております。

【表 1】5 月から 6 月 28 日にかけて JVN iPedia に公開された WordPress の脆弱性

最終更新日	ID	タイトル	CVSSv3	CVSSv2
2021/6/24	JVNDB-2020-013311	WordPress 用 Good Layers LMS プラグインにおける SQL インジェクションの脆弱性	9.8	7.5
2021/6/23	JVNDB-2021-000056 (JVN#63066062)	WordPress 用プラグイン WordPress Popular Posts におけるクロスサイトスクリプティングの脆弱性	5.4	3.5
2021/6/22	JVNDB-2021-000055 (JVN#93799513)	WordPress 用プラグイン「不動産プラグイン」シリーズにおけるクロスサイトスクリプティングの脆弱性	5.4	4
2021/6/21	JVNDB-2020-013152	WordPress 用 usc-e-shop プラグインにおける脆弱性	8.8	6.5
2021/6/18	JVNDB-2020-013078	WordPress 用 WeForms プラグインにおける CSV ファイル内の数式要素の中和に関する脆弱性	9.8	7.5
2021/6/17	JVNDB-2020-013038	WordPress 用 Import and export users and customers プラグインにおけるインジェクションに関する脆弱性	8	6
2021/6/17	JVNDB-2020-013037	WordPress 用 Easy Registration Forms プラグインにおけるインジェクションに関する脆弱性	8.8	6.8
2021/6/11	JVNDB-2021-000047 (JVN#70566757)	WordPress 用プラグイン Welcart e-Commerce におけるクロスサイトスクリプティングの脆弱性	6.1	4.3
2021/5/28	JVNDB-2020-012762	WordPress におけるクロスサイトリクエストフォージェリの脆弱性	4.3	4.3
2021/5/28	JVNDB-2020-012761	WordPress の wp-includes / meta.php の is_protected_meta における任意のファイルを削除される脆弱性	9.1	6.4
2021/5/28	JVNDB-2020-012760	WordPress におけるクロスサイトスクリプティングの脆弱性	6.1	4.3
2021/5/28	JVNDB-2020-012759	WordPress の wp-includes / functions.php の is_blog_installed における新しいインストールを実行される脆弱性	9.8	7.5

最終更新日	ID	タイトル	CVSSv3	CVSSv2
2021/5/28	JVNDB-2020-012758	WordPress の wp-includes/class-wp-xmlrpc-server.php における権限を取得される脆弱性	9.8	7.5
2021/5/28	JVNDB-2020-012757	WordPress における権限を取得される脆弱性	9.8	7.5
2021/5/28	JVNDB-2020-012756	WordPress におけるグローバル変数に関連付けられたクロスサイトスクリプティングの脆弱性	6.1	4.3
2021/5/28	JVNDB-2020-012755	WordPress におけるマルチサイトネットワーク上の無効なサイトからの埋め込みを誤って処理される脆弱性	7.5	5
2021/5/28	JVNDB-2020-012754	WordPress における wp-includes / Requests / Utility / FilteredIterator.php のデシリアライゼーションリクエストを誤って処理される脆弱性	9.8	7.5
2021/5/24	JVNDB-2020-012723	WordPress 用 Greenmart テーマにおけるクロスサイトスクリプティングの脆弱性	6.1	4.3
2021/5/11	JVNDB-2020-012507	WordPress 用 Loginizer プラグインにおける SQL インジェクションの脆弱性	9.8	7.5
2021/5/11	JVNDB-2020-012503	WordPress 用 cm-download-manager プラグインにおけるクロスサイトスクリプティングの脆弱性	6.1	4.3

4. 最新の深刻度が高い脆弱性情報

5 月 13 日に WordPress のバージョン 5.7.2 が公開されました。アップデートによって WordPress のプラグイン「PHPMailer」に対する脆弱性である CVE-2020-36326 および CVE-2018-19296 が修正されています。

CVE-2018-19296 は入力確認に関する脆弱性で、悪用された場合、情報を取得される、情報を改ざんされる、およびサービス運用妨害（DoS）状態にされる可能性があります。この脆弱性は 2018 年に修正されました。その後 2020 年に実施した修正により再発したのが CVE-2020-36326 です。いずれの脆弱性も、バージョン 5.7.2 で修正されています。

深刻度が緊急、重要レベルの内容ですので早期にアップデートを行う事を推奨します。

5. 攻撃の影響

WordPress の脆弱性を用いた攻撃により以下のような影響があります。

・パソコンのマルウェア感染

悪意のあるスクリプトを埋め込むことで、そのサイトを訪れたユーザが別のサイトに飛ばされ、そこから感染してしまう可能性があります。

・Web サイトの改ざん

サーバ内のディレクトリのアクセス権限が奪取され、サイトが改ざんされる可能性があります。

・情報の不正取得

偽サイトなどに誘導され個人情報を入力してしまうと、重要情報が漏洩する可能性があります。

WordPress 本体が攻撃されるとリモートで Web サイトの改ざんが可能になり、サイトからの情報をリモートで不正取得することができます。プラグインはとても便利ですが、プラグインに脆弱性の問題が発生するとそこを攻撃してきて悪用されます。プラグインが攻撃されてもそこから Web サイトの改ざんや情報の不正取得を容易にすることができます。

6. 攻撃への対策

WordPress の脆弱性を用いた攻撃に対しては以下の対策が有効となります。

・最新バージョンへのバージョンアップ

・セキュリティ機器等による攻撃の監視

・Web サイトの公開情報を最低限に抑える

WordPress は CMS としての技術的な情報が多く流通しており、使いやすさの点でメリットがあります。一方で攻撃者にとってもこの情報の多さは攻撃しやすい条件に繋がります。世界的に見て WordPress を使っているホームページが全体の 3 割と考えられており、非常に多くのユーザが存在することで攻撃対象として狙われやすいです。さらに、WordPress は共通の構造になっていることが多い点も攻撃をうけやすくなっている要因の 1 つと考えられます。また、WordPress の脆弱性は WordPress 本体以外にプラグインにも脆弱性が発見されることが多いです。2 章に参考情報として記載した過去のセキュリティニュースや 5 章の攻撃の影響にありますとおり、プラグインから攻撃されることもあります。

このように WordPress は便利な反面、攻撃されやすいことを十分に理解して今後もセキュリティ対策を万全にしておく必要があります。

7. 参考情報

・マイナビ

WordPress に緊急の脆弱性、直ちにアップデートを（2021/05/14 15:37 公開情報）

https://news.mynavi.jp/article/20210514-1888237/

・JVN

脆弱性対策情報データベース検索

https://jvndb.jvn.jp/

→上記 URL で「WordPress」のキーワードで検索してください。

8. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。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重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、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。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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/

※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