滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No.１３
今、注目のサイバーセキュリティに関する情報をお届けします。

「ＷｏｒｄＰｒｅｓｓ」の脆弱性について

Webサイト構築に使用されるオープンソースソフトウェア「WordPress」について、Wordfence社から脆弱性情報（CVE-2022-3180、CVSSスコア9.8（緊急））が公表されていますので、「WordPress」を使用して自社のWebサイトを構築されている事業者様は対策を御検討ください。

脆弱性の概要

今回公表された「WordPress」の脆弱性は、「WordPress」のプラグイン（拡張機能）「WPGateway」に関する脆弱性です。

「WPGateway」は、Webサイト管理者がサイトのバックアップやサイトにおいて使用する拡張機能の管理をまとめて設定できる拡張機能です。

今回公表された脆弱性を悪用すると、攻撃者が認証を回避して管理者権限を持つ不正なユーザーを追加することが可能となり、Webサイトを乗っ取ることができます。

攻撃の確認方法

自社のWebサイトに対する攻撃を確認する方法として、次の事項を確認してください。

- 管理者権限を持つユーザーに「rangex」が追加されているか。
- Webサイトのアクセスログに、「//wp-content/plugins/wpgateway/wpgateway-webservice-new.php?wp_new_credentials=1」に対するリクエストがあるか。

なお、上記のリクエストがログに記録されていた場合、この脆弱性を狙った攻撃を受けたことを示しますが、必ずしも、サイト内への侵入に成功したことを示すものではありません。

対　　策

今回公表されている脆弱性は、修正プログラムが出ていないゼロディ脆弱性と言われるものです。Wordfence社の一部製品には、攻撃を回避するためのファイアウォールルールが配付されている模様ですが、無料バージョンに対する修正プログラムは、今のところリリースされていません。

したがって、「WPGateway」プラグインを「WordPress」にインストールしてWebサイトを構築されている事業者様は、

- 修正プログラムがリリースされるまで「WPGateway」を削除する。
- 管理者権限を持つユーザーに「rangex」があれば、無効化する。
- 「WordPress」のバージョンを、組み込んでいる拡張機能を含めて最新のものにする。

などの対策を御検討ください。

なお、Webサイトの構築を外部に委託されている事業者様は、今回の脆弱性に対して確実な対応がなされているかを、今一度委託先に御確認ください。

被害が発生したり前兆事案を把握された場合は、該当システムを管理する担当者に連絡するほか、警察にも御一報ください。

≪あなたの暮らしを守る情報SHIG@≫　**「還付金詐欺」に注意！**

令和４年10月１日から、後期高齢者医療制度が変わります。本制度の見直しに伴って、

㊟ 電話や訪問での登録手続きや通帳等を預かることは絶対にありません！！

㊟ ＡＴＭ操作で還付金が払い戻しされることは、絶対にありません！！

滋賀県警察本部　サイバー犯罪対策課　０７７－５２２－１２３１（代表）