ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●WordPress人気プラグイン「Contact Form 7」に脆弱性、有害ファイルアップロードによる攻撃の可能性も？

https://contactform7.com/ja/2020/12/17/contact-form-7-532/
https://ja.wordpress.org/plugins/contact-form-7/

このニュースをザックリ言うと･･･

- 12月17日(日本時間)、WordPressにおいてお問合せフォーム機能を提供するプラグイン「Contact Form 7」においてファイルのアップロード機能に関する脆弱性が報告されています。

- 開発者からのリリースによれば、脆弱性の悪用により、理論上は「ホストサーバー上でスクリプトファイルとして実行される可能性のあるファイルをアップロードできるように」なるとされています。

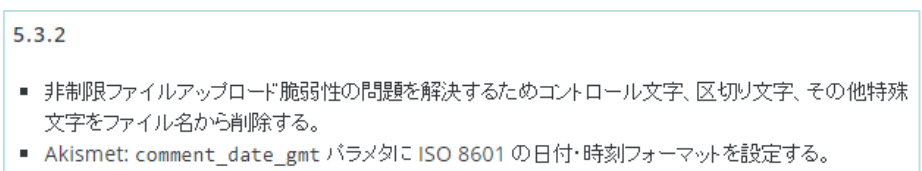
- 既に脆弱性を修正したバージョン5.3.2がリリースされており、使用しているサイトの管理者に対しアップデートが呼びかけられています。

AUS便りからの所感等

- 開発者のブログ(https://ideasilo.wordpress.com/2020/12/19/professional-work/)において紹介されている、WordPressのセキュリティプラグイン「Wordfence」の開発元が行った検証によれば、当該プラグインにおける複数の被害軽減策により、脆弱性を実際に悪用することは困難とされている模様です(例えば、ファイルが実際にアップロードされるのは極めて短時間、かつランダムな名前の一時ディレクトリ下に配置されるとのことです)。

- Webサーバーの設定を安全なものにする(例えばディレクトリリストを表示する機能を無効化する等)ことにより、今回のケース以外でも脆弱性の悪用を困難にする場面が出てくると思われます(ただし著名なWebサーバーでも、例えばApacheとnginxで設定方法が異なり、「.htaccess」ファイルによるディレクトリ毎の設定はApacheでしか使えないこと等に注意が必要です)。

- ともあれ、WordPressは本体や人気のあるプラグインに脆弱性が報告され、アップデートが推奨されるケースが多くあり、例えば9月にも「File Manager」に脆弱性が報告されたことがあります(AUS便り 2020/09/14号参照)ので、最初にサイトを構築してから放置することは決してせず、管理画面から随時アップデートを行う体制を整えることが肝要であり、加えて様々な攻撃への防御のために、セキュリティ関連のプラグインあるいはWordPressに特化したWAFを導入すること等も是非とも検討すべきでしょう。



●セディナ・OMC等クレジットカード各社を騙るフィッシング多発

https://www.itmedia.co.jp/news/articles/2012/15/news070.html
https://www.antiphishing.jp/news/alert/cedyna_omc_20201214.html

このニュースをザックリ言うと・・・

- 12月14日(日本時間)、フィッシング対策協議会より、SMBCファイナンスサービスが発行するセディナカード・OMCカードを騙るフィッシングが確認されたとして注意喚起が出されています。

- フィッシングメールの一例として、件名が「【セディナカード・OMC】カードご利用確認」等、本文では「ご本人様のご利用かどうかを確認させていただきたい」「カードのご利用を一部制限」等の文言が書かれ、https://www.cedyna.co.jp.●●●●.com/ というURLの偽サイトに誘導、アカウント情報・カード情報および個人情報を詐取するものが挙げられています。

- 同協議会からは11月にUCS・アプラス・ポケットカード、12月に入っても同じくUCS・オリコ・三井住友カードを騙るフィッシングへの注意喚起が相次いで出されています。

AUS便りからの所感

- 前述した注意喚起を見る限り、11月以降、これまでターゲットになることが少なかった様々なブランドのクレジットカードに関するフィッシングが目立ってきています。

- 同協議会から、12月18日にUFJ銀行を騙るものと、宅配便の通知を騙るいわゆるスミッシングについても注意喚起が出る等、その他のフィッシングも依然多種多様に出回っていますので、不審なメール・SMSのリンクをクリックしない、リンク先のサイトで個人情報を入力しない、そして利用しているサービスのサイトにはブックマークからアクセスすることを常に心掛けましょう。


フィッシング対策協議会
Council of Anti-Phishing Japan

セディナカード・OMC カードをかたるフィッシング (2020/12/14)　緊急情報

2020年12月14日

概要

セディナカード・OMC カードをかたるフィッシングの報告を受けています。

メールの件名

【セディナカード・OMC】カードご利用確認
セディナカード・OMCカードご利用確認

上記以外の件名も使われている可能性があります。

詳細内容

セディナカード・OMC カードをかたるフィッシングの報告を受けています。

1. 2020/12/14 11:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。

2. このようなフィッシングサイトにて、アカウント情報 (ユーザ ID、パスワード)、クレジットカード情報 (カード番号、カード有効期限、セキュリティコード)、お支払い口座の口座番号下 4 桁、暗証番号、個人情報 (氏名、生年月日、電話番号) 等を、絶対に入力しないよう、ご注意ください。

メール本文

＋拡大する

●年末年始における情報セキュリティに関する注意喚起、IPAより発表

https://www.ipa.go.jp/security/topics/alert20201217.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となる年末年始を迎えるにあたり、12月17日(日本時間)にIPAより、情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- IPAは毎年のこの時期あるいはゴールデンウィークや夏季休暇の時期に注意喚起を行っております(https://www.ipa.go.jp/security/measures/vacation.html)が、今年からは新型コロナウイルス感染症の影響によるテレワーク・Web会議・自宅でのPC利用増加も鑑み、そういった環境における注意事項についても取り上げられています。

AUS便りからの所感

- JPCERT/CCも同様に毎年4・12月の定例として近日発表を行うとみられます(現時点の最新は4月:https://www.jpcert.or.jp/newsflash/20200041401.html)が、こういったセキュリティ機関の呼びかけでは、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントが挙げられており、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- 注意喚起等をいつご覧になったかに拘わらず、その時点で点検すべきことは様々ですので、以後も、ゴールデンウィークや夏季といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。


IPA

年末年始における情報セキュリティに関する注意喚起

最終更新日：2020年12月17日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人が年末年始の長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

最近では外出自粛等の影響により、逆に家でパソコンなどを利用する時間が長くなり、ウイルス感染やネット詐欺被害のリスクが高まることも考えられます。

これらのような事態とならないよう、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

■長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■日常的に実施すべき情報セキュリティ対策