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サイトの管理者アカウント奪取、改ざんされ偽ブラウザー配信サイトに…攻撃に注意喚起

https://news.mynavi.jp/techplus/article/20240305-2897927/
https://blog.sucuri.net/2024/03/new-wave-of-socgholish-infections-impersonates-wordpress-plugins.html

### このニュースをザックリ言うと･･･

- 3月1日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、WordPressサイトに不正アクセスし、マルウェアをダウンロードさせるよう改ざんする攻撃が活発化しているとして注意喚起が出されています。

- 攻撃はWordPress管理者アカウントに不正ログインし、Chromeブラウザーのアップデートと偽ってマルウェア「SocGholish」をダウンロードさせるものとされています。

- SocGholishによるブラウザーアップデートを装ってのマルウェア感染活動は2023年の時点で度々活動が確認されていますが、Sucuri社によれば「先週後半」即ち2月下旬から活動の活発化がみられたとしています。

### AUS便りからの所感等

- Sucuri社によれば、SocGholishによる改ざんの際、以前はデータベースの改変を行っていましたが、今回は偽のWordPressプラグインをインストールするという手口をとっていたとしています。

- Webサイト管理者側においては管理者アカウントのパスワードに推測されやすいものを使わない等の原則を徹底する他、WordPressにおいては必ずセキュリティ機能を提供するプラグインを導入し、適宜不正ログイン試行の記録等を確認して警戒する、加えて可能であればWAFやサーバー上のファイル改ざん検知ソリューション等の導入も検討するようにしてください。

- また閲覧者側においても、使用しているソフトウェア自身に自動更新機能やアップデートの有無を確認する機能があるものについては必ずそれを利用すること、またサーチエンジンの検索結果のうち広告として表示されるものについては特に偽サイトの報告が目立っているため、アンチウイルスおよびブラウザーのアンチフィッシング機能は必ず有効化し、信頼できる情報源からのリンクを辿る等の自衛策をとることが重要です。

TECHF Powered by マイナビニュース

### WordPressサイトを偽のブラウザ配信サイトに変えるサイバー攻撃に警戒を

掲載日 2024/03/05 12:08　　著者：後藤大地

Sucuriは3月1日(米国時間)、「New Wave of SocGholish Infections Impersonates WordPress Plugins」において、WordPressサイトを侵害してマルウェア「SocGholish」を配布する新しいキャンペーンを特定したと伝えた。このキャンペーンではWordPressの管理者アカウントを侵害し、悪意あるプラグインをインストールすることでマルウェアの配布サイトに改ざんするという。

#### マルウェア「SocGholish」の特徴

マルウェア「SocGholish」は別名「偽のブラウザ配信」と呼ばれており、侵害したWebサイトからブラウザアップデートを装って配布される。マルウェアの種別は遠隔操作型トロイの木馬(RAT: Remote Administration Trojan)とされ、少なくとも2017年からJavaScriptフレームワークを使用して配布されていることが確認されている。

# ●Microsoft・Adobeより月例のセキュリティアップデートリリース

https://forest.watch.impress.co.jp/docs/news/1575865.html
https://msrc.microsoft.com/blog/2024/03/202403-security-update/
https://forest.watch.impress.co.jp/docs/news/1575909.html

## このニュースをザックリ言うと･･･

- 3月13日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5035845(ビルド 19045.4170)およびWindows 11 23H2 KB5035853(ビルド22631.3296)となります。

- 同日にはAdobe社からもExperience Manager・Premiere Pro等に対するセキュリティアップデートがリリースされています。

## AUS便りからの所感

- MSについては、今回修正された脆弱性を悪用する「ゼロデイ攻撃」は確認されなかったとのことです。

- Windows 11において2月の月例セキュリティアップデートのインストールが完了しないという不具合が報告されていた模様ですが、今回解決したとのことです。

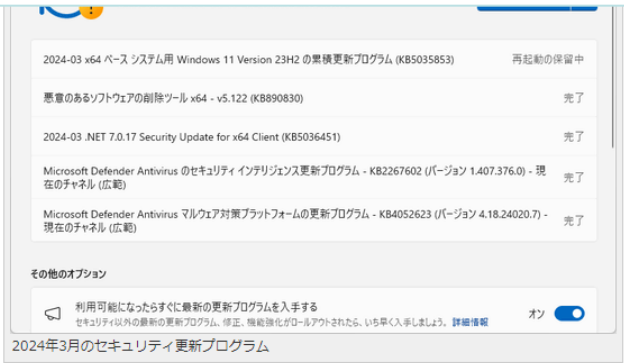
- ともあれ今後発生し得る新たな攻撃に備え、確実にアップデートを適用すること、それまでに発生する攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。

Impress Watch

**2024年3月の「Windows Update」、59件の脆弱性へ新たに対処 ～「USB 80Gbps」にも対応**

［モバイル デバイス］設定ページ、Androidの撮影通知といった新要素も

樽井 秀人　2024年3月13日 09:38



2024年3月のセキュリティ更新プログラム

米Microsoftは3月12日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで59件の脆弱性が新たに対処されている。

# ●FortiOSに危険度の高い脆弱性…2月発表分の未対策機器は世界15万台か

https://www.fortiguard.com/psirt/FG-IR-23-328
https://news.mynavi.jp/techplus/article/20240311-2902835/
https://www.bleepingcomputer.com/news/security/critical-fortinet-flaw-may-impact-150-000-exposed-devices/
https://twitter.com/Shadowserver/status/1765742604933574865

## このニュースをザックリ言うと･･･

- 3月13日(日本時間)、Fortinet社より、同社のFortiOSに存在する脆弱性3件の情報が発表されました。

- 非常に危険度の高い脆弱性としてCapative Portalに存在する脆弱性(CVE-2023-42789・CVE-2023-42790)が挙げられ、外部から機器を乗っ取られる恐れがあるとされており、他にもSSL-VPNのWebポータルに存在する脆弱性(CVE-2024-23112)等2件が挙げられています。

- 3件の脆弱性が修正されたのはFortiOSバージョン7.0.14・7.2.7・7.4.2等とされ、最新バージョンにアップデートされているか確認が推奨されます。

- 一方で同9日、米IT系メディアBleeping Computerより、外部に公開されているFortinet社製機器のうち、2月に同社が発表した脆弱性「CVE-2024-21762」(AUS便り 2024/02/14号参照)に対応していないものが約15万台存在するとの調査結果が報じられています。

## AUS便りからの所感

- FortiOSのバージョンは2月の脆弱性に対応した7.0.14・7.2.7・7.4.3等が最新で、2月中に最新に更新していれば、今回発表された分の脆弱性には既に対応しています。

- 前述の調査結果では、日本国内でも同様の機器が約1万台残っているとされています。

- 自動更新機能が有効でなく(ただしデフォルトで有効となるのは7.2.6以降と比較的限られています)、最新バージョンへの追随が1ヶ月以上遅れ、脆弱性を外部から悪用される恐れがある危険な状態となっているのを解消するため、まずは手動であっても最新バージョンにアップデートし、以後のアップデートについても基本的に自動更新を有効にして計画的に実行することが重要です。

TECH+ Powered by マイナビニュース

**Fortinet FortiOS、FortiProxyの緊急の脆弱性、国内約1万台が未対策**

掲載日 2024/03/11 08:42　著者：後藤大地

Bleeping Computerは3月8日(米国時間)、「Critical Fortinet flaw may impact 150,000 exposed devices」において、インターネットに公開されているFortinet製品のうち約15万台が既知の緊急の脆弱性「CVE-2024-21762」に対して脆弱なまま修正されていないと報じた。

この脆弱性は悪用されるとリモートの認証されていない攻撃者により任意のコードを実行される可能性がある。また、米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA: Cybersecurity and Infrastructure Security Agency)はすでに悪用が確認されているとして、脆弱性カタログ(KEV: Known Exploited Vulnerabilities Catalog)にこの脆弱性を登録している。