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。

●FortiOSに危険度の高い脆弱性…速やかにアップデートを

https://www.ipa.go.jp/security/security-alert/2023/alert20240209.html
https://www.fortiguard.com/psirt/FG-IR-24-015

このニュースをザックリ言うと・・・

- 2月9日(日本時間)、Fortinet社より、同社のFortiOSに存在する脆弱性4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、SSL-VPNに存在する脆弱性(CVE-2024-21762)と、fgfmdサービス(FortiManagerによる機器管理時の通信用)に存在する脆弱性(CVE-2024-23113)の2点が挙げられており、それぞれ外部から機器を乗っ取られる恐れがあるとされています。
- 特にCVE-2024-21762について、IPAやJPCERT/CC等からも注意喚起が出されている他、同社では既に脆弱性を悪用した攻撃も確認されているとし、速やかに対策バージョンへの更新を強く推奨しています。

AUS便りからの所感等

- FortiOSやFortiProxyでは、ここ数年の間にもSSL-VPNに関する脆弱性が度々報告され、これを悪用して組織内ネットワークに侵入されたことによるとみられる情報漏洩等の事案も発生しています。
- 4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・7.4.3、FortiProxyバージョン7.0.16・7.2.9・7.4.2等で、他の同社製品にも影響するものや、古いバージョン(FortiOS 7.0系等)では全ての脆弱性について修正されていないものもあり、各組織で導入している製品やバージョン、利用している機能をもとに十分に情報を確認してください。
- FortiOSではバージョン7.2.6以降ファームウェアの自動アップデート機能がデフォルトで有効になっており、万一意図しない場面でのアップデートを避けたい場合を除き、可能な限り有効化しておくべきですが、デフォルトの設定ではアップデートのリリース確認から適用まで3日のタイムラグがあるため、必要に応じ設定の変更、安全なバージョンにアップデートされたかの確認、あるいは手動アップデート実行等の検討も望ましいでしょう。

IPA

Fortinet 製 FortiOS SSL VPN の脆弱性対策について(CVE-2024-21762)

公開日：2024年2月9日
最終更新日：2024年2月14日

概要

Fortinet 社より、FortiOS の SSL VPN 機能に関する脆弱性が公表されました。

この FortiOS SSL VPN において、リモートからのコード実行の脆弱性が確認されています。

本脆弱性を悪用された場合、認証されていない遠隔の第三者によって細工したリクエストを送信され、任意のコードまたはコマンドを実行される可能性があります。

今後被害が拡大する可能性があるため、早急に対策を実施してください。

影響を受けるシステム

--- 2024年 2 月 14 日更新 ---

・FortiOS バージョン 7.4.0 から 7.4.2
・FortiOS バージョン 7.2.0 から 7.2.6
・FortiOS バージョン 7.0.0 から 7.0.13
・FortiOS バージョン 6.4.0 から 6.4.14
・FortiOS バージョン 6.2.0 から 6.2.15
・FortiOS バージョン 6.0 系の全てのバージョン
・FortiProxy バージョン 7.4.0 から 7.4.2
・FortiProxy バージョン 7.2.0 から 7.2.8
・FortiProxy バージョン 7.0.0 から 7.0.14
・FortiProxy バージョン 2.0.0 から 2.0.13
・FortiProxy バージョン 1.2 系の全てのバージョン
・FortiProxy バージョン 1.1 系の全てのバージョン
・FortiProxy バージョン 1.0 系の全てのバージョン

●1月フィッシング報告件数は85,827件、フィッシングサイト数の増加傾向続く

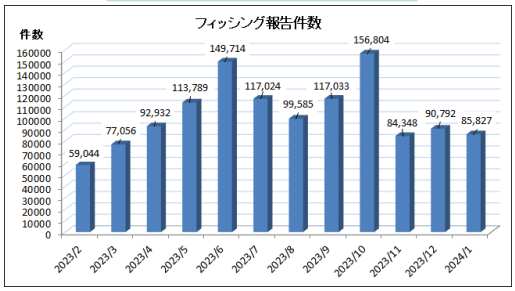
https://www.antiphishing.jp/report/monthly/202401.html

このニュースをザックリ言うと・・・

- 2月14日(日本時間)、フィッシング対策協議会より、1月に寄せられたフィッシング報告状況が発表されました。
- 1月度の報告件数は85,827件で、12月度(https://www.antiphishing.jp/report/monthly/202312.html)の90,792件から4,965件減少しています。
- フィッシングサイトのURL件数は19,486件で12月度(17,172件)から2,314件増加、悪用されたブランド件数は74件で12月度(80件)から6件減少となっています。
- 最も多く報告されたのはETC利用照会サービスを騙るフィッシングで報告数全体に対する約18.0%、次いで報告が多かった三井住友カード、Amazon、マイナポイント事務局、エポスカードと合わせて約55.5%、さらに1,000件以上報告された16ブランドまで含めると約91.3%を占めたとのことです。

AUS便りからの所感

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



- 報告件数は2023年10月度で156,804件を記録したのを最後に激減し、ここ3ヶ月間は85,000件前後～90,000件強で推移が続いています。
- フィッシングサイトURL件数は12月度に急増して以降も増加傾向が続いており、フィッシングサイトへのリダイレクト元として、Cloudflare Workersで付与できるサブドメインを悪用するケースが全体の約61.4%(12月度 約37.2%)に上るとのことです。
- 悪用されたブランド上位のうちETC、Amazonについては1月初旬に多く報告されたものの、中旬以降は減少し、しばらく報告が少なかったブランドの報告が増えたとしています。
- フィッシングメール・サイトからの自衛策として、これまでも度々言われていることですが、不審なメールが届いた場合には、同協議会や日本データ通信協会の迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/news/alert.html)等の団体が発表する情報あるいはソーシャルネットワークでの報告がないか確認すること、利用しているサービスのサイトへは事前に登録したブラウザーのブックマーク等からアクセスするよう心掛けること等、慎重な行動が肝要です。

●アニメ・Webメディア・選管等SNSアカウント乗っ取り相次ぐ

https://www.itmedia.co.jp/news/articles/2401/31/news109.html
https://www.itmedia.co.jp/news/articles/2401/30/news104.html
https://www.itmedia.co.jp/news/articles/2402/07/news097.html
https://www.itmedia.co.jp/news/articles/2401/31/news152.html

このニュースをザックリ言うと・・・

- 1月下旬以降、X(旧Twitter)をはじめとするSNSでのプロモーション等アカウントの乗っ取りが相次いでいます。
- 1月28日(日本時間)、漫画・アニメ作品「攻殻機動隊」のXアカウントが第三者に乗っ取られたことが発表され、同30日に復旧しています。
- 1月29日、Webメディア「ITMedia」の「ITmedia Mobile」「スマートジャパン」各Xアカウントが乗っ取られたと発表、のち2月6日までに復旧しています。
- 2月6日には愛知県選挙管理委員会のXアカウントが一時乗っ取られ、バナー等がネットゲームのものに差し替えられる事態が発生しましたが、こちらも同7日に復旧しました。

AUS便りからの所感

ITmedia NEWS

- 「攻殻」については作品内での事件の年月日に合わせて様々なプロモーションを行っていたことから、アカウントの乗っ取りも同様のプロモーションであると誤解される一幕もありました。
- この他、2023年末にカメラレンズメーカーのシグマ社が「SIGMA Japan」のInstagramアカウントを乗っ取られており、1月31日に同じアカウント名で新たにアカウントを作成したと発表しています。
- パスワード認証において、他と共有していない強固なパスワードを設定することはもちろん、XのようにTOTP(ワンタイムパスワード)等を用いての2要素認証を提供しているサービスではこちらも有効化することにより、アカウントの保護を心掛けるようにしてください(フィッシングによってパスワードを奪取しようとするケースも多く、2要素認証はそこでの不正なログイン阻止に有用です)。

「攻殻機動隊」公式Xが乗っ取り被害　不正アクセス受け

2024年01月29日 11時55分 公開　[ITmedia]

講談社のヤングマガジン編集部は1月29日、「攻殻機動隊」公式X（旧Twitter）アカウント（@thegitsofficial）が28日朝から不正アクセスを受けて乗っ取られたため、利用を中止していると発表した。再開についてX社と調整しているという。

不正アクセスによる被害報告はないが、引き続き他の公式SNSを含めて調査し、セキュリティ強化を進めていくという。復旧予定が決まれば公式サイトなどで告知する。