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。

●Fortinet社製品のセキュリティアップデート…FortiOS・FortiProxyの脆弱性に特に注意

https://www.jpcert.or.jp/at/2025/at250003.html
https://www.fortiguard.com/psirt/FG-IR-24-535

このニュースをザックリ言うと･･･

- 1月15日(日本時間)、Fortinet社より、同社各製品(FortiOS・FortiProxy・FortiManager他)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。

- このうちFortiOS・FortiProxyの脆弱性「CVE-2024-55591」について、管理者権限を奪取される可能性がある等非常に危険度が高く、既に悪用も確認されているとして同社およびJPCERT/CC等より注意喚起が出されています。

- CVE-2024-55591の影響を受けるのはFortiOS 7.0.0～7.0.16およびFortiProxy 7.0.0～7.0.19・7.2.20～7.2.12とされ、修正バージョンであるFortiOS 7.0.17、FortiProxy 7.0.20・7.2.13へのアップデートが呼び掛けられています(回避策として、Web管理インタフェースの無効化あるいはアクセス元IPアドレスの制限設定も提示されています)。

AUS便りからの所感等

- 同社からは計34件の脆弱性に関するアドバイザリーが発表され、FortiOSについては上記を含め14件が関係しています。

- 脆弱性によっては、例えばFortiOS 7.0・7.2系のような最新でないバージョン系列では修正されず、より新しい系列へのアップデートが必要になるもの、アップデート後に設定の追加が必要になるものもあるため、Fortinet社や販売店からの情報をもとに必要なアップデート・対策の実施を計画してください。

- FortiOSやその他のベンダー製ネットワーク機器においては、VPN機能の脆弱性を悪用され、組織内ネットワーク、さらにはVPNで接続された別のネットワークへと侵入されるケースも度々報告されており、アップデートの実施はもちろん、回避策でも示されているように機器やそのサービスポート等へ不特定多数からアクセスされないよう可能な限りフィルタリング設定をかけること、さらには稼働の必要がないサービスがあれば無効化すること等も重要です。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

Fortinet製FortiOSおよびFortiProxyにおける認証回避の脆弱性（CVE-2024-55591）に関する注意喚起

最終更新: 2025-01-15

JPCERT-AT-2025-0003
JPCERT/CC
2025-01-15

I. 概要

2025年1月15日（現地時間）、FortinetはFortiOSおよびFortiProxyにおける認証回避の脆弱性（CVE-2024-55591）に関するアドバイザリを公開しました。本脆弱性により、遠隔の第三者によって細工されたリクエストを送信され、super-adminの権限を取得される可能性があります。Fortinetは、本脆弱性の悪用が報告されていることを公開しています。

Fortinet
Authentication bypass in Node.js websocket module
https://www.fortiguard.com/psirt/FG-IR-24-535

また、本脆弱性との直接の関係に言及はありませんが、米セキュリティ組織Arctic Wolf Networksが1月10日（現地時間）に公表したFortinet製品の侵害事案の調査記事では、2024年11月16日から12月末までの間に、特定の分野や組織を限定せずに攻撃が行われたと述べています。

Arctic Wolf Networks
Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls
https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/

●複数回やり取り後にマルウェア送信…警察庁・NISCがサイバー攻撃に注意喚起

https://www3.nhk.or.jp/news/html/20250108/k10014687711000.html
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

このニュースをザックリ言うと･･･

－1月8日(日本時間)、警察庁と内閣サイバーセキュリティセンター(NISC)より、「MirrorFace」と呼ばれるサイバー攻撃グループによる、国内組織(企業・省庁)の関係者に対しマルウェア添付メールを送り付ける「標的型メール攻撃」等が確認されたとして注意喚起が出されています。

－発表によれば、攻撃には中国の関与が疑われており、2019年以降大きく3種類の攻撃キャンペーンが確認されているとのことです。

－例えば2019年12月～2023年7月頃に把握したとする攻撃では、当時の国際情勢に関連したもの(「日米同盟」「台湾海峡」「ロシア・ウクライナ戦争」)等を件名に用いたメールを送り、相手と複数回やり取りを行った後でマルウェア添付メールを送るという手口がとられていたとしています。

AUS便りからの所感

－これまでにも「ビジネスメール詐欺(BEC)」と呼ばれる詐欺行為等で、対象が実際に取引している相手になりすましたり、ある程度の期間のやり取りで安心させてから攻撃を始める手口が使われています。

－今回の発表では、攻撃に際し、本来はWindowsのセキュリティ機能である「Windows Sandbox」を悪用するケース(サンドボックス内でマルウェアを実行することにより、痕跡を調査しづらい状況にする)、コードエディタ「Visual Studio Code(VS Code)」を悪用するケース(対象PCにVS Codeを不正にインストールし、バックドアを設置する)等が挙げられています。

－システム管理者のみならずユーザーにおいても、可能な限り発表資料を読み込み、攻撃の手口を熟知した上で、不審な相手に騙されないよう慎重に行動すること、またマルウェアへの感染を阻止するためアンチウイルス・UTMによる防御を固めることが肝要です。

NHK

サイバー攻撃グループが省庁や企業狙い不審メール 中国関与か

2025年1月8日 15時09分

警察庁と内閣サイバーセキュリティセンターは、中国の関与が疑われるサイバー攻撃グループ「ミラーフェイス」が、日本の安全保障の情報を扱う省庁や民間企業などを狙って不審なメールを送りつけるなどのサイバー攻撃を仕掛けているとして、注意を呼びかけています。

警察庁によりますと、「ミラーフェイス」と呼ばれるサイバー攻撃のグループは、2019年から2024年にかけて、日本の外務省や防衛省、政治家、それに情報通信や半導体を扱う民間企業などを標的にサイバー攻撃を行っていて、使われたマルウエアなどの分析から、中国の関与が疑われることが判明したということです。

● Microsoft、月例のセキュリティアップデートリリース…Chromeも新バージョンリリース

https://forest.watch.impress.co.jp/docs/news/1654426.html
https://msrc.microsoft.com/blog/2025/01/202501-security-update/
https://forest.watch.impress.co.jp/docs/news/1654438.html

このニュースをザックリ言うと･･･

－1月15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 KB5049981(ビルド 19045.5371)、11 23H2 KB5050021(ビルド 22631.4751)および11 24H2 KB5050009(ビルド 26100.2894)等となります。

－またこの日はChromeブラウザーも新しいバージョン132(132.0.6834.83/84)がリリースされる等、各社のセキュリティアップデートの集中日(いわゆる「パッチチューズデー」)となっています。

AUS便りからの所感

Impress Watch

－MSの月例アップデートではCVEベースで159件の脆弱性が修正されており、Hyper-V関連の脆弱性3件が既に悪用を確認、Accessに関する3件を含む計5件が攻撃手法が明らかにされており、この他11件の脆弱性が特に危険度が高いと評価されているとのことです。

－「パッチチューズデー」は米国時間での第2火曜日となることから、2025年は今月の他10月についても、8日(日本時間で第2水曜日)ではなく、15日(第3水曜日)がリリースとなります(https://msrc.microsoft.com/blog/2024/11/securityupdatereleaseschedule2025/)。

－また22日にはOracleからもJavaやMySQL等に対する4半期毎のセキュリティアップデートがリリース予定である等、こういった定期的にリリースされるパッチの適用について必要に応じ十分に計画すること、社内における パッチの展開・適用完了までに発生し得る攻撃に対しアンチウイルス・UTM等による防衛を怠りなく実施することが肝要です。

2025年最初の「Windows Update」、159件の脆弱性に対処 ～悪用あり、致命的なものも多数

かならず適用を

樽井 秀人　2025年1月15日 09:15

米Microsoftは1月14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159件（サードパーティーのものも含めれば161件）の脆弱性が新たに対処されている。