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のSSL-VPN機能に脆弱性、内部ネットワーク侵入の恐れも…速やかにアップデートを

https://www.jpcert.or.jp/at/2022/at220032.html
https://www.ipa.go.jp/security/ciadr/vul/alert20221213.html
https://www.fortiguard.com/psirt/FG-IR-22-398

このニュースをザックリ言うと･･･

- 12月12日(現地時間)、大手セキュリティベンダーのFortinet社より、同社のFortiOSに危険度の高い脆弱性(CVE-2022-42475)が確認されたとして注意喚起が出されています。
- 脆弱性はSSL-VPN機能に存在し、リモートからの悪用により、FortiOSが動作する機器上で任意のコード・コマンドが実行される恐れがあるとされます。
- 同社では脆弱性を修正したFortiOSの最新バージョンをリリースしており、また既に脆弱性を悪用した攻撃が確認されているとして、速やかにアップデートを行うよう呼び掛けています。
- 当該脆弱性については、IPAおよびJPCERT/CCからも同様に注意喚起が出されています。

AUS便りからの所感等

- 同社から脆弱性の存在が発表されたのは、FortiOS バージョン6.2.0～6.2.11、6.4.0～6.4.10、7.0.0～7.0.8、7.2.0～7.2.2と、FortiOS-6K7K バージョン6.0.0～6.0.14、6.2.0～6.2.11、6.4.0～6.4.9、7.0.0～7.0.7です。
- また脆弱性が修正されたのは、FortiOS バージョン6.2.12、6.4.11、7.0.9、7.2.3と、FortiOS-6K7K バージョン6.0.15、6.2.12、6.4.10、7.0.8となり、これらのバージョンまたはそれ以降へのアップデートが推奨されます。
- VPN機器における今回のような脆弱性の悪用は、機器の乗っ取り、さらには内部ネットワークへの侵入につながる恐れがあり、FortiOSにおいては、2019年5月にも今回同様SSL-VPN機能の脆弱性を修正するアップデートがリリースされた後、2020年11月に依然対策がされていないホストの情報が攻撃者のフォーラムで公開される事態(AUS便り 2020/11/30号参照)が発生しています。
- 今回も未対策の機器が早々に攻撃者に発見されてターゲットとなることが考えられるため、特にSSL-VPN機能を使用している場合は必ず早急にアップデートを行うこと、またVPNアクセスのためのアカウント情報を奪取される恐れもあるため、アクセスログ等を確認し、アップデートまでの間に攻撃を受けた様子が見られた場合はアカウント情報の変更を行うことを強く推奨致します。

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

FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起

最終更新: 2022-12-13

ツイート　メール

JPCERT-AT-2022-0032
JPCERT/CC
2022-12-13

I. 概要

2022年12月12日（現地時間）、FortinetはFortiOS SSL-VPNにおけるヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関するアドバイザリ（FG-IR-22-398）を公開しました。本脆弱性が悪用されると、認証されていない遠隔の第三者が、細工したリクエストを送信し、任意のコードやコマンドを実行する可能性があります。

Fortinet
FortiOS - heap-based buffer overflow in sslvpnd
https://www.fortiguard.com/psirt/FG-IR-22-398

Fortinetは、本脆弱性を悪用する攻撃を確認しています。影響を受ける製品を利用している場合、Fortinetが提供する最新の情報をご確認の上、対策の適用に加え、脆弱性を悪用する攻撃の被害を受けていないか確認するための速やかな調査実施を推奨します。

● 11月フィッシング報告件数は70,204件…引き続き減少傾向に

https://www.antiphishing.jp/report/monthly/202211.html

このニュースをザックリ言うと・・・

- 12月6日(日本時間)、フィッシング対策協議会より、11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。

- 11月度の報告件数は70,204件で、10月度(https://www.antiphishing.jp/report/monthly/202210.html)の78,126件から7,922件減少しています。

- フィッシングサイトのURL件数も24,114件と、10月度(29,604件)から5,490件の減少、フィッシングに悪用されたブランド数は87件で10月度(89件)から2件減少となっています。

- Amazonを騙るフィッシングが全体の約36.5%と急増(10月度20.9%)、以下国税庁・楽天+楽天カード・セゾンカードおよびえきねっとを騙るものと合わせて全体の約74.9%を占めたとのことです。

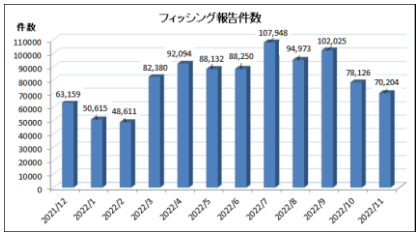
AUS便りからの所感

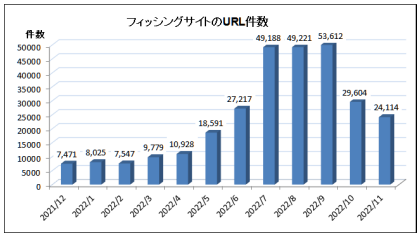
- 報告件数が8万件を超えていた3～9月度から一転、2か月連続で減少傾向を見せていますが、過去には12月・1月といった年末年始に急増したケースもあり、油断はできません。

- フィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は、.topが約36.9%でトップ、次いで.org(約23.0%)と.ly(約18.1%)、以下.com、.cn、.icu、.shopが上位に挙げられています。

- スマートフォンユーザーを狙い、モバイルネットワーク以外からは見れないフィッシングサイトもあるとしており、フィッシングからの効果的な回避のため、利用しているWebサイトへのアクセスは事前に登録したブックマークや公式のモバイルアプリからアクセスするよう心掛けるとともに、PCはもちろんスマホ・タブレットにおいてもアプリストアやソーシャルネット等で評価されているセキュリティアプリのインストールを検討することを推奨致します。

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





●年末年始における情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/topics/alert20221213.html

このニュースをザックリ言うと・・・

- 12月13日(日本時間)、IPAより、年末年始を迎えるにあたっての、情報セキュリティに関する注意喚起が出されました。

- 多くの企業・組織において、この時期に従業員等が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

- IPAは毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っており(https://www.ipa.go.jp/security/measures/vacation.html)、他にも経済産業省(METI)・総務省・警察庁および内閣官房内閣サイバーセキュリティセンター(NISC)が今年から連名で同様の注意喚起を行っています。

AUS便りからの所感

IPA

- 注意喚起の内容は、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から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっています。

- 併せて、多く寄せられている相談事例として「公的機関を装った偽ショートメッセージ」および「スマートフォンの偽セキュリティ警告から自動継続課金アプリへのインストール誘導」についても改めて注意が呼び掛けられています。

- 挙げられているセキュリティ対策の内容は毎回大きく異なるようなものではなく、この他にも長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/measures/everyday.html)」として別途まとまっており、常日頃において準備・点検を行うよう意識していくことが肝要です。


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：2022年12月13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

被害に遭わないためにもこれらの対策の実施をお願いします。

ランサムウェアによるサイバー攻撃被害に関する相談や報告が企業や組織から寄せられています。
インターネットに接続された機器・装置類に対し、脆弱性の悪用などが原因による外部からの不正アクセス事案が報告されています。
リモートデスクトップサービス（RDP）の認証を突破されたり、VPN装置のアップデートが行われておらず侵入されたという事例が多くあります。
インターネットからアクセス可能な装置全体について、アクセス制御が適切にできているか、認証が突破される可能性はないか、脆弱性は解消されているかといった点を、今一度確認することを推奨します。

- 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について