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社製品の脆弱性に未対応のホスト情報、攻撃者フォーラムで公開か…JPCERT/CCが注意喚起

https://www.jpcert.or.jp/newsflash/2020112701.html

このニュースをザックリ言うと･･･

- 11月27日(日本時間)、JPCERT/CCより、Fortinet社製機器のOS「FortiOS」において2019年に修正された脆弱性(CVE-2018-13379)について、対応を行っておらず影響を受ける可能性があるとされるホストの情報が攻撃者のフォーラムで公開されているとして、注意喚起が出されています。

- 脆弱性が存在するのはFortiOS バージョン5.4.6～5.4.12、5.6.3～5.6.7、6.0.0～6.0.4で、SSL VPNサービスが有効であるときに影響を受けるとされ、悪用により機器上の任意のファイルを読み取られる恐れがあるとのことです。

- 注意喚起によれば、同19日以降未対策ホストの情報が公開されていることを確認しており、情報にはIPアドレスや平文のパスワード含むSSL VPNのアカウント情報が含まれている他、国内ホストのIPアドレスも対象となっているとのことです。

AUS便りからの所感等

- JPCERT/CCでは対象組織に対し情報提供を順次行うとしており、アップデートの対応や、回避策としてSSL VPNサービスの無効化または認証における多要素認証の導入を推奨しています。

- 2019年8月に脆弱性の詳細が発表された時点から、脆弱性が存在するホストの探索ないし脆弱性の悪用が始まっていたとされており、JPCERT/CCではこれ以後にアップデートを行った場合、既にSSL VPNのアカウント情報が奪取されている恐れを考慮し、パスワードの変更を行うよう呼び掛けています。

- クライアントPCやサーバーに比べ、ネットワーク機器のファームウェアは、特に自動更新機能がなかったり無効にされていると、管理が行き届かず何年も古いバージョンのままである可能性や、機器によってはサポートが終了してアップデートが提供されない可能性もあることに注意し、組織内の全ての機器について存在を把握し、定期的な管理が行われる体勢を整えること、あるいは業者による保守サポートが行われるUTM等についても利用を検討することが重要です。

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

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

最終更新: 2020-11-27

ツイート　メール

CyberNewsFlash一覧

(1) 概要

JPCERT/CC は、2020年11月19日以降、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストに関する情報が、フォーラムなどで公開されている状況を確認しています。当該情報は、FortiOS の既知の脆弱性 (CVE-2018-13379) の影響を受けるとみられるホストの一覧です。この一覧は、攻撃者が脆弱性を悪用可能であることを確認した上で作成したものとみられ、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザーアカウント名や平文のパスワードなどの情報が含まれているとのことです。

JPCERT/CC は、当該情報に日本の IP アドレスが含まれていることを確認し、連絡可能な対象組織へ、直接または関係組織を通じた情報提供を順次行っています。もし、当該製品を使用しており、脆弱性の影響を受けるバージョンおよび条件で稼働している場合は、公開されてしまった認証情報や脆弱性を悪用した攻撃の被害を受ける可能性があるため、以降に記載の対策や侵害有無確認などを実施することを推奨いたします。

(2) 脆弱性の詳細

FortiOS には、任意のファイル読み取りの脆弱性 (CVE-2018-13379) があります。脆弱性が悪用されると、遠隔の第三者が当該製品から任意のファイルを読み込む可能性があります。対象となるバージョンは次のとおりです。

●EU機密ビデオ会議に記者乱入、SNS写真から暗証番号入手

https://www.afpbb.com/articles/-/3317269

このニュースをザックリ言うと・・・

- 11月20日(現地時間)、オランダのマルク・ルッテ首相より、EU国防相機密ビデオ会議に第三者がログインした事態を受け、オンライン上のセキュリティを強化するよう注意喚起が出されました。

- オランダ国防相のTwitterアカウントに投稿された画像にビデオ会議のアカウント情報の一部が掲載されていたことを同国メディアの記者が発見し、会議への不正ログインに成功したことによるものです。

- その後犯罪行為の可能性を指摘された記者はすぐにログアウトし、会議は中止、問題となった画像も削除されたとのことです。

AUS便りからの所感

- 問題となった画像にはアカウントのIDおよび6桁の暗証番号のうち5桁が読み取れる状態になっていたとのことです。

- 手指が映った画像から指紋認証を不正に突破されたり、鍵の画像から合鍵の複製が可能だったり(正式にサービスとしている所もあるようです)といった話題は、特にSNSの普及によって注意すべき事柄として度々取り上げられています。

- 電子的・物理的な認証の突破以外に、顔写真の瞳に映っていた内容から撮影場所を特定してストーキングが行われる等も問題となっており、写真や画像投稿時のモザイクやスタンプでの加工等はセキュリティ面でも重要であると心がけるべきでしょう。

AFP BB News

EU機密ビデオ会議に記者乱入、SNS写真から暗証番号入手

2020年11月22日 10:30 発信地：ハーグ/オランダ [オランダ, ヨーロッパ]

【11月22日 AFP】オランダのマルク・ルッテ（Mark Rutte）首相は20日、国防相のツイッター（Twitter）アカウントに投稿された情報を使って一人の記者が欧州連合（EU）の国防相機密ビデオ会議にログインしたことを受け、オンライン上のセキュリティーを強化するよう警告した。

オランダの民放RTLニュース（RTL Nieuws）によると、記者のダニエル・フェルラーン（Daniel Verlaan）氏は、同国のアンク・バイレフェルト（Ank Bijleveld）国防相のツイッターに投稿された写真からログイン用アドレスと暗証番号の一部を入手し、EU諸国の国防相らが参加する機密会議にログイン。

隔離中のバイレフェルト氏は在宅で勤務しており、同氏が投稿した写真には卓上に置かれた書類も写り込んでいた。フェルラーン氏は書類に書かれていた6桁の暗証番号のうち5桁を写真から読み取れることに気付き、「その後まもなく会議にログインできた」という。

この様子を撮影した映像では、黒いTシャツを着たフェルラーン氏が笑顔で他の国防相らに手を振る様子が映し出されている。

●「使ってはいけないパスワードTop200」2020年版発表、1位はやはり「123456」

https://gigazine.net/news/20201120-most-common-passwords-2020/
https://nordpass.com/most-common-passwords-list/

このニュースをザックリ言うと・・・

- 11月18日(現地時間)、パスワード管理ツール「NordPass」の開発元より、「Top 200 most common passwords of the year 2020」と題し、使ってはいけないとされるパスワードのランキングが発表されました。

- ランキングは、最もよく「使用された」「流出した」および「クラッキングのために試行された」頻度に基づいており、1位は「123456」、以下トップ10までは「123456789」「picture1」「password」「12345678」「111111」「123123」「12345」「1234567890」「senha」となっています。

- また、ランキングの発表とともに、強力なパスワードを作成する際の注意として「辞書の単語・数字の組み合わせ・キーボード上で隣接する組み合わせの文字列は使用しない」「電話番号・生年月日・名前等完全に機密ではないかもしれない個人情報に基づいてパスワードを選択しない」「決して複数のアカウントでパスワードを使い回さない」等を挙げています。

AUS便りからの所感

GIGAZINE

- NordPassによるランキングは2019年から開始されたものですが、トップ10のうち3位「picture1」と10位「senha」(ポルトガル語で「パスワード」を意味します)は今回初めてランクインしたものとなっています。

- 同様のランキングは他のパスワード管理ツールの開発元やセキュリティ企業・機関からも発表されていますが、数字の羅列や「password」のような簡単な単語およびその組み合わせが上位に入る傾向は、どのランキングでも何年もの間共通したものとなっています。

- ランキングには「Time to crack it(ハッシュ化されたパスワードのリストに対し元のパスワードが割り出されるまでの時間と思われます)」も掲載されていますが、トップ10の多くが1秒以内、「picture1」でも3時間程度で割り出される模様です。

- ともあれ、今回の発表以前に様々なアカウント奪取を目論む攻撃者が使用する脆弱なパスワードの辞書には既に載っている可能性が高く、Web・メールサービスはもちろん、あらゆる場面において使わないよう注意しましょう。

2020年に最も使われたパスワードは何だったのか？常連に加えて新顔も登場

データ流出によって2020年に漏えいしたパスワード2億7569万9516件の分析によって、2020年版の「最も使われたパスワード」ランキングが公開されました。1位はこれまでさまざまな調査でトップを飾ってきた「123456」ですが、これまでにみられなかった新たなパスワードも登場しています。