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。

●7月のMS定例アップデートで修正未完了の脆弱性発表、緩和策適用呼び掛け

https://www.ipa.go.jp/security/security-alert/2023/0712-ms.html
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

このニュースをザックリ言うと･･･

- 7月12日(日本時間)、マイクロソフト(以下・MS)より同社各製品(Windows・Officeその他)に対するセキュリティアップデートがリリースされ、IPA等からも適用が呼び掛けられています。
- MSやIPA等からは、今回のセキュリティアップデートでは修正されていない、OfficeおよびWindowsのHTMLコンポーネントの脆弱性(CVE-2023-36884)も存在するとして、同時に注意喚起が出されています。
- 不正なOfficeファイルを開くことにより、PCを乗っ取られる可能性もあるとし、緩和策の適用が推奨されています。

AUS便りからの所感等

- 当該脆弱性は、6月に欧米政府機関に対し発生した攻撃で悪用された、いわゆる「ゼロデイ脆弱性」とされています。
- MSから挙げられている緩和策情報によれば、「Microsoft Defender for Office」を利用している場合は脆弱性を悪用する添付ファイルから保護されるとし、他にも「Defender for Endpoint」での設定の追加や、レジストリの設定が挙げられています。
- ともあれMSから当該脆弱性へのセキュリティアップデートがリリースされるまでの間に攻撃に対し無防備とならないよう、MS製・サードパーティー製に拘らずアンチウイルスやUTM等による防御を固めることが重要です。

IPA

Microsoft 製品の脆弱性対策について(2023年7月)

公開日：2023年7月12日
最終更新日：2023年7月12日

注釈： 追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2023年7月12日（日本時間）に Microsoft 製品に関する脆弱性の修正プログラムが公表されています。
これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生するおそれがあります。

この内 CVE-2023-32046、CVE-2023-32049、CVE-2023-35311、CVE-2023-36874、CVE-2023-36884 の脆弱性について、Microsoft 社は悪用の事実を確認済みと公表しており、今後被害が拡大するおそれがあるため、至急、修正プログラムを適用してください。なお、CVE-2023-36884 については緩和策を適用してください。

対策

1.脆弱性の解消 - 修正プログラムの適用

Microsoft 社から提供されている修正プログラムを適用して下さい。
Windows Update の利用方法については以下のサイトを参照してください。

Windows Update の利用手順 – Windows 11 の場合
Windows Update の利用手順 – Windows 10 の場合

●FortiOS・FortiProxyに重大な脆弱性、アップデートを

https://www.npa.go.jp/bureau/cyber/pdf/Vol.10cpal.pdf
https://www.fortiguard.com/psirt/FG-IR-23-183

このニュースをザックリ言うと･･･

- 7月12日(日本時間)、Fortinet社より、同社の各種製品に存在する脆弱性2件の情報が発表されました。
- このうちFortiOS・FortiProxyのSSLディープインスペクション(HTTPS暗号化通信を復号して分析する機能)に存在する脆弱性(CVE-2023-33308)については、不正なパケットにより、機器上で任意のコード・コマンドが実行される可能性がある、特に危険度が高いものとされており、同社製品を扱う代理店各社や警察庁等からも注意喚起が出されています。。
- Fortinet社ではFortiOS等について既に脆弱性を修正した最新バージョンをリリースしている他、回避策も案内しています。

AUS便りからの所感

- 当該脆弱性(CVE-2023-33308)はFortiOS 7.0系・7.2系およびFortiProxy 7.0系・7.2系に存在し、SSLディープインスペクションとプロキシモードが同時に有効な場合に発現するとのことです。
- FortiOSバージョン7.0.11・7.2.4およびFortiProxyバージョン7.0.10・7.2.3で対策されていますが、6月にセキュリティアップデートがリリース(AUS便り 2023/06/13号参照)された際にFortiOSバージョン7.0.12・7.2.5およびFortiProxyバージョン7.0.10・7.2.4にアップデートしている場合は既に対策済みとなります。
- 使用している機能が有効でない場合にアップデートを保留している組織も少なからずあるとみられますが、未発表の脆弱性が対策され、後日発表されるケースが度々あるようですので、新しいバージョンがリリースされるたびに適用し、可能な限り最新バージョンに保つことを推奨致します。

●メール誤送信が発生する6つの原因･･･NECが発表

https://scan.netsecurity.ne.jp/article/2023/07/10/49646.html
https://jpn.nec.com/cybersecurity/blog/230630/index.html

このニュースをザックリ言うと･･･

- 6月30日(日本時間)、NECより、「電子メール誤送信の発生原因と対策」と題した記事が同社ブログで発表されました。
- 記事では2021年度における個人情報漏洩の事故原因の37.0%がメール誤送信で、2020年度に比べ誤送信件数が約1.5倍に増加しているというJIPDECの調査結果が取り上げられています。
- メール誤送信の原因として「タイプミス」「自動補完機能(オートコンプリート)による誤入力」「類似した名前・アドレスの混同」「CCとBCCの誤用」「メーリングリストの不適切な設定」「ファイルの誤添付」の6つを挙げるとともに、対策としては送信者・第三者・システムのそれぞれで操作ミスを見つけることと、また送信前の他にも送信後(メールサーバー上から外部に配送する前)においての対策についても取り上げています。

AUS便りからの所感

- 当AUS便りでも主に「CCとBCCの誤用」が原因の事例の他、「***@gmail.com」を「***@gmai.com」と誤って入力した事例等を取り上げています。
- 7月17日(現地時間)には、米政府からのメールが米国防総省と下位組織が使用するドメイン名「.mil」のメールアドレスではなく、マリ国のドメイン名「.ml」のアドレスに長年送信されていたことも報じられています(https://nordot.app/1053809275408777666)。
- 記事で挙げられるチェック方法は「送信者による目視」といった最もシンプルなものからシステム側での「確認ダイアログ」「遅延送信」「ポリシーによるチェック」まで広範囲にわたっており、最もコストがかからないからと人間によるチェックだけに決して依存せず、必ずシステムによるチェックの採用を意識し、誤送信が発生しない仕組みを整えることが重要です。


調査・レポート・白書・ガイドライン／調査・ホワイトペーパー
2023.7.10 Mon 8:00
メール誤送信 6 大発生原因 ～ NEC 考察
日本電気株式会社（NEC）は6月30日、電子メール誤送信の発生原因と対策について同社セキュリティブログで解説している。NECサイバーセキュリティ戦略統括部セキュリティ技術センターの山田英史氏が執筆している。
シェア ツイート 送る
日本電気株式会社（NEC）は6月30日、電子メール誤送信の発生原因と対策について同社セキュリティブログで解説している。NECサイバーセキュリティ戦略統括部セキュリティ技術センターの山田英史氏が執筆している。
日本情報経済社会推進協会（JIPDEC）の2021年度「個人情報の取扱いにおける事故報告集計結果」によると、個人情報漏えいの事故原因の37.0%は「メール誤送信」で最多となり、2020年度と比較し約1.5倍に増加していることからも、注意が必要な状況になっているとしている。