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。

● Windowsに未修正の脆弱点…Office文書ファイルからの攻撃も確認か

https://forest.watch.impress.co.jp/docs/news/1349516.html
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
https://www.ipa.go.jp/security/ciadr/vul/20210908-ms.html

このニュースをザックリ言うと･･･

- 9月7日(現地時間)、米マイクロソフト社(以下・MS)より、Windowsに存在する未修正の脆弱性「CVE-2021-40444」について注意喚起が出されています。

- 脆弱性はInternet Explorer(IE)のレンダリングエンジン「MSHTML」に存在し、Windows 7・Server 2008以降から現行のWindows10(および先日リリースされたServer 2022)にまで影響するとしています。

- MSでは、細工したOffice文書(Word・Excel等)から脆弱性を悪用する攻撃を既に確認しているとのことで、JPCERT/CCやIPAからも相次いで警告が出されています。

AUS便りからの所感等

- 9月14日(日本時間)時点でMSから修正パッチはリリースされておらず、回避策として、レジストリの編集により、IEにおいてActiveXコントロールのインストールを無効化すること等を挙げていますが、これらは完全な対策とはならないとする情報もあり、根本的な対策は翌15日の月例パッチまたはそれ以降における緊急パッチのリリースにおいて行われることになるでしょう。

- 別の回避策として挙げられている「保護ビュー」によるOffice文書の閲覧はこれまでにも不正なマクロによる攻撃の回避に実績があるものの、警告に表示される「編集を有効にする」をクリックすると攻撃が成立してしまう恐れがあるため、信頼できる相手以外からの添付ファイルは開かない、また開いた場合でも「編集を有効する」はクリックしないよう十分に注意を払うことが肝要です。

- また、Windows10に標準搭載されているMicrosoft Defender Antivirusでは(9月2日リリースのセキュリティインテリジェンスのバージョン1.349.22.0以上において)脆弱性に対する攻撃を検知するようになっており、アンチウイルスベンダー各社のプロダクトでも順次対応される模様ですので、今回に限らずアンチウイルスソフトやUTMの導入、メーラー・ブラウザー等の各種セキュリティ機能を確実に有効にすること、そしてアンチウイルスソフトとそのパターンファイル等は必ず最新に保つことを心掛けましょう。

Impress Watch

Windowsにゼロデイ脆弱性 ～リモートからコードを実行される恐れ

修正パッチは未公開。Microsoftは回避策を発表

長谷川 正太郎　2021年9月8日 13:00

米Microsoftは9月7日（現地時間）、Windowsに未修正の脆弱性「CVE-2021-40444」が存在することを発表した。深刻度は同社の基準で5段階中2番目に高い「Important」。すでに悪用が確認されているという。

脆弱性が存在するのは、Windows 7/Server 2008以降のWindows。32bit/64bit版のWindows 10 バージョン 21H1やWindows Server 2022はもちろん、ARM64版のWindows 10も含まれる。

脆弱性の内容は、「Internet Explorer」のレンダリングエンジン「MSHTML」の欠陥により、リモートからコードを実行されてしまうというもの。特別な細工をした「Microsoft Office」文書を使用した攻撃が確認されているとのこと。

●ランサムウェア対策のデータバックアップは「3-2-1-1-0ルール」で…Veeam社提案

https://ascii.jp/elem/000/004/067/4067991/

このニュースをザックリ言うと・・・

- 9月2日(現地時間)、バックアップ等データ保護ソリューションを提供する米Veeam Software社より、「5 Ransomware Protection Best Practices(ランサムウェア対策 5つのベストプラクティス)」と題したホワイトペーパーについての説明会が行われました。

- これまでランサムウェアによる暗号化からデータを保護するためのバックアップルールとして提唱されていた、「最低でも3つのデータコピー」を「2種類のメディア」に保存し、「1つはオフサイト(別の場所)に保管する」という「3-2-1ルール」について、現在の脅威状況においては不十分であるとし、これに「1つの不変性(書き換え不可能な)バックアップ／オフラインバックアップ」と「バックアップ／リストアのエラーはゼロ」を加えた「3-2-1-1-0ルール」を提唱しています。

- 同社では、バックアップしたデータまで暗号化されてしまうことのないよう、不変性バックアップの確保を特に重要視しており、またリストアできないエラーが発生しないようバックアップ取得後の自動的なテストの実施も必要としています。

AUS便りからの所感

- 発表ではオンプレミス環境における同社や同社のパートナーによるバックアップソリューションを紹介するとともに、パブリッククラウド環境でも不変性ストレージが提供されていることを取り上げています。

- 7月には国内製粉業大手において、ランサムウェアによるとみられるデータ暗号化での大規模なシステム障害が発生しており(AUS便り 2021/08/18号参照)、ここでもバックアップからのデータ復旧に失敗していた可能性が指摘されています。

- システムの可用性と完全性の維持のため、データのバックアップと、そこからの復旧を確実なものとするよう、有用なソリューションの検討と、バックアップ～復旧のテストの随時実施が重要です。

効果的なランサムウェア対策のためのホワイトペーパーを公開、新たな「3-2-1-1-0ルール」を提唱
「バックアップの“3-2-1ルール”はランサム対策として不十分」Veeamが語る
2021年09月02日 13時30分更新　文●大塚昭彦／TECH.ASCII.jp

Veeam Softwareは2021年9月2日、新たに公開したホワイトペーパー「5 Ransomware Protection Best Practices(ランサムウェア対策 5つのベストプラクティス)」についての記者説明会を開催した。

説明会には同ホワイトペーパーを執筆した製品戦略担当シニアディレクターのリック・バノーバー氏が出席し、サイバーセキュリティフレームワークに沿った対策や新たに提唱する「3-2-1-1-0ルール」の重要性、そしてそれを実現できるVeeam製品の機能や優位性について紹介した。

●数百万台のMicrosoft IISが脆弱なバージョンのまま運用

https://news.mynavi.jp/article/20210911-1969359/
https://cybernews.com/security/millions-of-microsoft-web-servers-powered-by-vulnerable-legacy-software/

このニュースをザックリ言うと・・・

- 9月9日(現地時間)、リトアニアのセキュリティニュースメディアCyberNewsより、世界中で数百万台のMicrosoft IIS Webサーバーが脆弱なバージョンのまま稼働しているとする調査結果が発表されました。

- IISは現時点でWebサーバー市場の12.4%程度のシェアを持っているとされていますが、発表によれば、推定で700万台を超えるIISがレガシーバージョンのままで、100万台以上のサーバーが昨年開発終了となったバージョンのIISを使用しているとのことです。

- これら脆弱なIISサーバーの殆どはアジアと北米にあり、国別では中国が最も多く、次いで米国・香港・韓国となっているとのことです。

AUS便りからの所感

- 脆弱なIISサーバーの多くは、企業や組織による適切な管理の対象となっておらず、Windowsクライアント上で開発環境・試験環境で立てられたきりのものも少なからずあると推測されます。

- それらのサーバーが意図せず外部の第三者からアクセス可能な状態となっていることもまた問題ですが、そうでなかったとしても、内部ネットワークにひとたびマルウェアが侵入した場合、サーバーにも脆弱性を悪用されて侵入され、外部への攻撃の踏み台とされる恐れがあります。

- サポートが切れたOSやソフトウェアが使い続けられることがないよう、計画的にアップグレードを行うよう検討し、特に万が一古いOSやソフトウェアを使い続ける必要がある場合には、意図しない場所との通信が行われないよう、UTM等を用いて他のPCと隔離されたネットワークに配置すべきでしょう。

数百万台のMicrosoft IISが脆弱なバージョンのまま運用

2021/09/11 16:39　著者：後藤大地

CyberNewsは9月9日(米国時間)、「Millions of Microsoft web servers powered by vulnerable legacy software | CyberNews」において、世界中で数百万台に上るMicrosoft IISがサポートされていない脆弱なバージョンのまま運用されていると伝えた。こうしたサーバはサイバー犯罪者にとって格好の標的であるとされており、注意が呼びかけられている。

CyberNewsの研究者らによる主な調査結果は次のとおり。

- 数百万台に上るMicrosoft IISがサポートされていない脆弱なバージョンのまま運用されている（推定で700万台を超えるMicrosoft IISがレガシーバージョンのまま）
- 100万台以上のサーバが、昨年、Microsoftによって開発終了となったIISのバージョンを使用している
- 脆弱なMicrosoft IISのほとんどのサーバはアジアと北米に存在している。中国が最も多く、これに米国、香港、韓国が続いている