— AUS（アルテミス・ユーザ・サポート）便り 2020/03/30号 —
https://www.artemis-jp.com

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に未修正の脆弱性、ファイルのプレビューで攻撃の可能性

https://forest.watch.impress.co.jp/docs/news/1242590.html
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/ADV200006

このニュースをザックリ言うと・・・

- 3月23日(現地時間)、マイクロソフト(以下、MS)より、Windowsに存在する未修正の脆弱性について注意喚起が出されています。

- 脆弱性はエクスプローラーでのプレビュー機能等に影響し、細工されたドキュメント・メディアファイルをプレビューするだけでマルウェアに感染する等の可能性があるとのことです。

- MSでは攻撃を受ける可能性を抑止するため、パッチがリリースされるまでの間に実行すべき回避策をいくつか提示しています(ただし、Windows 10 バージョン1703以降については問題を緩和する要素があり、システム全体を乗っ取ることは不可能としています)。

AUS便りからの所感等

- 先日Windows 10のファイル共有等に関するプロトコルの脆弱性が定例外のパッチで修正された(AUS便り 2020/3/16号参照)ばかりですが、今回問題となるのはWindows 8.1や7等も含まれ、非常に影響範囲が広いものとなっています。

- 特にWindows 7をターゲットとした標的型攻撃が確認されているとの情報がMSから出ている上、有償延長サポート(ESU)を購入しないかぎり修正パッチがリリースされても適用できないものとみられるため、7を使い続けているPCでは必ず何らかの緩和策を実施してください。

- Windows 8.1以降におけるパッチのリリースが定例となる4/9か、それ以前になるかは不明ですが、いずれにせよ緩和策の実行とともに、アンチウイルスやUTMによる防御を確実に行い、メールやWebサイトからの不審なドキュメント・メディアファイルのダウンロードについて平生から十分注意を払うことが重要です。

Microsoft

セキュリティ更新プログラム ガイド > 詳細

ADV200006 | Type 1 フォント解析のリモートでコードが実行される脆弱性

セキュリティ アドバイザリ

公開日: 2020/03/23 | 最終更新日 : 2020/03/27

このページのトピック
- 概要
- 悪用可能性指標
- ソフトウェア更新
- 問題を緩和する要素
- 回避策
- よく寄せられる質問
- 謝辞
- 免責
- 更新履歴

マイクロソフトは、Adobe Type Manager Library のパッチ未適用の脆弱性を悪用する可能性のある Windows 7 ベースの限定的な標的型攻撃を確認しており、セキュリティ更新プログラムがリリースされるまで、お客様のリスクを軽減する次のガイダンスを提供しています。また、業界パートナーの取り組みに感謝し、これらの限定的な攻撃に関する情報を開示する 7 日間のタイムラインを遵守しています。

Windows Adobe Type Manager ライブラリが特別に細工されたマルチマスター フォントの Adobe Type 1 PostScript 形式を不適切に処理する場合に、Microsoft Windows に 2 つのリモートでコードが実行される脆弱性が存在します。

攻撃者がこの脆弱性を悪用する手段は複数考えられます。攻撃者はこの脆弱性を悪用するために、たとえば、特別に細工されたドキュメントを開いたり、Windows プレビュー ウィンドウで表示したりするようにユーザーを誘導する可能性があります。

マイクロソフトはこの脆弱性を認識しており、修正プログラムに取り組んでいます。Microsoft ソフトウェアのセキュリティの脆弱性を解決する更新プログラムは、通常、毎月第 2 火曜日 (米国時間) の定例リリースで公開されます。この予測可能なスケジュールにより、パートナーは品質を保証し、IT 担当者は計画を立てることができるため、お客様にとって信頼性の高い安全な選択肢として Windows エコシステムを維持できます。この脆弱性の影響を受けるオペレーティング システムのバージョンを以下に示します。このリスクを緩和する方法については、緩和策と回避策を参照してください。

注: 2015 年にリリースされた最初のバージョンで緩和策が導入され、Windows 10 を実行しているシステムの脅威は低くなっています。

●2014～2019年のフィッシングサイトの傾向、JPCERT/CC発表

https://news.mynavi.jp/article/20200324-1001823/
https://blogs.jpcert.or.jp/ja/2020/03/phishing2019.html

このニュースをザックリ言うと・・・

- 3月19日(日本時間)、JPCERT/CCより、2014～2019年に同組織に報告されたフィッシングサイトの推移・傾向について発表されました。

- 報告される件数は2016年には200件/月だったものが、2017年頃から徐々に増加、2019年6月まで600件前後で推移していたのが7月には1,000件を超え、以後もその勢いが続いているとのことです。

- また、HTTPSを使用しているフィッシングサイトも2017年から急増、2018・2019年には全体の約半数で使用されるまでになっています。

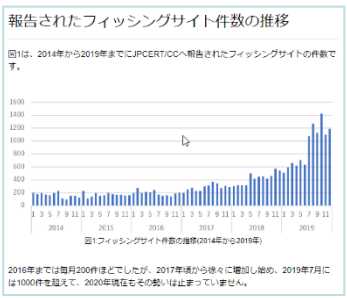
AUS便りからの所感

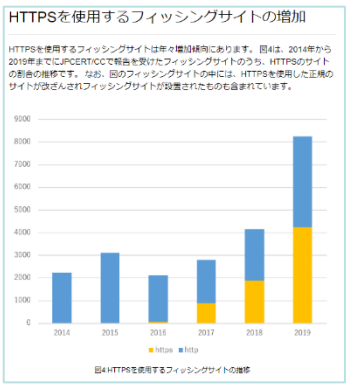
- 業種別では、世界的には2017年よりAmazonやApple IDを騙るサイトが急増したことによりEコマースの割合が最も大きくなっており、国内ではSMS(ショートメール)の悪用による金融機関を騙るサイトの急増が目立っているとのことです。

- 当AUS便りで取り上げるフィッシングサイトはHTTPSを使用していないものもまだ散見されますが、2016年に登場したSSL証明書を無料で発行するサービスが、フィッシングサイトでも利用されてHTTPSの使用率急増に寄与していることは明らかで、「HTTPSを使用しているか否か」は既に正規サイトを見分ける基準にはなり得ていません。

- アンチウイルスやUTMおよびWebブラウザーのアンチフィッシング機能を有効化した上で、利用している各種Webサービスについてはブックマークに登録し、メールのリンクからではなくそこからアクセスすることにより、フィッシングサイトの回避を行うよう心がけましょう。

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





●ラック、「テレワーク時のセキュリティ7つの落とし穴」公開

https://news.mynavi.jp/article/20200319-999007/
https://www.lac.co.jp/lacwatch/service/20200318_002153.html

このニュースをザックリ言うと・・・

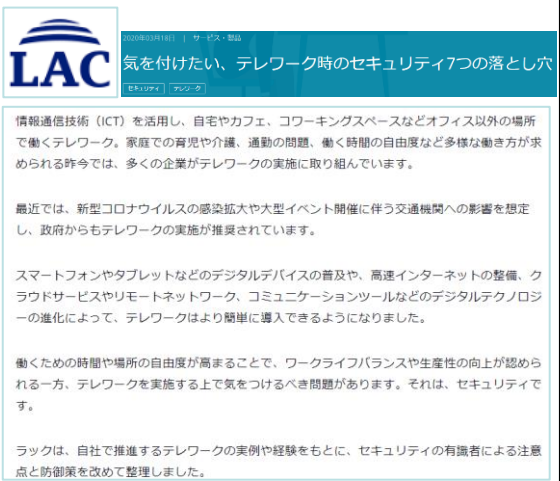
- 3月18日(日本時間)、国内大手セキュリティ企業のラック社より、「気を付けたい、テレワーク時のセキュリティ7つの落とし穴」と題した記事が発表されました。

- 記事で挙げられている落とし穴(あるいは注視しておくべき点)は、「ウイルスの入り口対策(PCに内蔵された通信機能を使用する場合に攻撃者やマルウェアが外部から直接攻撃を試みる可能性、等)」「ニセの会議招集メール(を含むフィッシング・標的型攻撃メール、等)」「パソコンののぞき見による情報漏えい(いわゆるショルダー・ハック)」「公共の場所でのWeb会議(顧客の名前・プロジェクトの具体的な情報を話してしまう可能性、等)」「公共無線LANやクニセの無料無線LAN(SSIDおよびキーが本物と同じに設定されているアクセスポイントによる通信の盗聴)ラウドでの共有設定」「ネットワーク機器やパソコンのアップデート」「」となっています。

AUS便りからの所感

- 新型コロナウイルス対策としてのテレワーク(リモートワーク)実施の増加に伴い、3月13日にはUS-CERT等の米政府機関より、特にVPNの利用で発生しえるセキュリティリスクへの注意喚起が出されており(AUS便り2020/3/23号参照)、こちらも注目すべき事柄が挙げられています。

- ラック社が挙げている7点の多くは、テレワークという言葉がより強く意識される以前から、ノートPCを外部に持ち歩いて仕事をするケースにおいて度々指摘されてきたポイントでもあり、そういった外部での作業をするか否かに関わらず必ず目を通し、今後テレワークを行う必要が生じたときに十分に備えて頂ければ幸いです。


LAC
2020年03月18日 | サービス・製品
気を付けたい、テレワーク時のセキュリティ7つの落とし穴
セキュリティ テレワーク

情報通信技術（ICT）を活用し、自宅やカフェ、コワーキングスペースなどオフィス以外の場所で働くテレワーク。家庭での育児や介護、通勤の問題、働く時間の自由度など多様な働き方が求められる昨今では、多くの企業がテレワークの実施に取り組んでいます。

最近では、新型コロナウイルスの感染拡大や大型イベント開催に伴う交通機関への影響を想定し、政府からもテレワークの実施が推奨されています。

スマートフォンやタブレットなどのデジタルデバイスの普及や、高速インターネットの整備、クラウドサービスやリモートネットワーク、コミュニケーションツールなどのデジタルテクノロジーの進化によって、テレワークはより簡単に導入できるようになりました。

働くための時間や場所の自由度が高まることで、ワークライフバランスや生産性の向上が認められる一方、テレワークを実施する上で気をつけるべき問題があります。それは、セキュリティです。

ラックは、自社で推進するテレワークの実例や経験をもとに、セキュリティの有識者による注意点と防御策を改めて整理しました。