— AUS（アルテミス・ユーザ・サポート）便り 2021/03/22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月例アップデートの不具合、2度の定例外リリースで解消か

https://forest.watch.impress.co.jp/docs/news/1313004.html
https://forest.watch.impress.co.jp/docs/news/1313336.html

このニュースをザックリ言うと･･･

- 3月19日(日本時間)、マイクロソフト(以下・MS)より、Windowsの月例セキュリティアップデートで報告されていた不具合を修正した定例外アップデートがリリースされました。

- 同10日にリリースされたWindows 10 2004/20H2向けパッチ「KB5000802」および同1909向けパッチ「KB5000808」等において、一部メーカー製複合機での印刷時等にブルースクリーン(BSoD)が発生する不具合が報告されたことを受け、同16日にこの不具合を修正したとする定例外のアップデート「KB5001567」「KB5001566」等がリリースされました。

- しかしこのアップデートの適用後、今度はページが正常に印刷されない場合があるという別の不具合が報告され、さらなる定例外アップデートとなる「KB5001649」「KB5001648」等がリリースされています(10より前のWindows 8.1/7等においてもこれらの不具合に対応したアップデートが後日リリースされています)。

AUS便りからの所感等

- KB5001649等はリリース後に一時Windows Updateから取り下げられ、「Microsoft Update カタログ」からダウンロードする必要がありましたが、現在は再びWindows Updateで配信されています(ただし「オプションの品質更新プログラム」として表示され、「ダウンロードしてインストール」をクリックしてインストールする必要があります)。

- 特にWindows 10においては毎月のセキュリティアップデートにおいて何らかの不具合の報告が続いている一方、修正される脆弱性は毎回多岐にわたり、リリース時点で既に脆弱性の悪用が確認されていたケースも珍しくありません。

- 今回問題となったKB5000802等も本来は速やかに適用されるべきセキュリティアップデートであり、不具合発生時に「更新を7日間一時停止」にしていたユーザーにおいては是非とも「更新プログラムのチェック」をクリックして更新を再開し、かつKB5001649等最新のアップデートを確実に適用することを強く推奨致します。

- セキュリティアップデートの適用こそが脆弱性への根本的な対応となるとはいえ、不具合によって業務に支障が出る恐れから適用を遅らせる選択をするケースは少なからず存在するでしょうが、その間隙をぬって脆弱性を狙われる可能性を抑止するには、普段からアンチウイルスやUTM等による防御を固めているかにかかっていると言えます。

Impress Watch

Windowsの印刷機能に再び問題 ～一部アプリ・プリンターで印刷時に画像が欠けるなどの現象

9日公開の月例セキュリティパッチや15日公開の緊急パッチを適用した環境で発生

樽井 秀人　2021年3月18日 17:17

米Microsoftは3月17日（現地時間、以下同）、Windowsの印刷機能に再び問題が発生していることを明らかにした。今月のセキュリティパッチ（9日公開）や、それに起因する印刷機能のブルースクリーン（BSoD）エラーに対処した緊急パッチ（15日公開）を適用した環境で発生しているという。

同社によると、以下のような現象が報告されているとのこと。

- バーコード、QRコード、ロゴなどのグラフィックス要素など、ドキュメントの一部が黒一色で印刷されたり、欠けたりする
- テーブル（表）を印刷した際に、罫線が欠ける。文字の配置や書式に問題が発生することもある
- 一部のアプリやプリンターで印刷すると、白紙のページやラベルが表示される

Microsoft、印刷の不具合に対処したパッチを緊急リリース

まずはWindows 10向け。Windows 7/8.1などの旧バージョン向けは後日提供

樽井 秀人　2021年3月19日 20:15

米Microsoftは3月18日（現地時間、以下同）、Windowsの印刷機能で発生している不具合を修正する更新プログラムを定例外でリリースした。現在、“Windows Update”や“Microsoft Update カタログ”から入手可能だ。

今月のセキュリティパッチ（9日公開）や、それに起因する印刷機能のブルースクリーン（BSoD）エラーに対処した緊急パッチ（15日公開）を適用した環境において、印刷結果が意図したものと異なる現象が多数報告されている。具体的には、ドキュメントに含まれるグラフィックス要素が欠けたり、黒塗りになったり、テキストの位置やスタイルが正常に印刷されなかったり、白紙のページが印刷されるといったケースが確認されているようだ。

● Exchange Serverの脆弱性を狙った攻撃報告…4日で10倍に、MSは回避ツールリリース

https://news.mynavi.jp/article/20210316-1810424/
https://www.itmedia.co.jp/news/articles/2103/17/news136.html

このニュースをザックリ言うと･･･

- 3月11日(現地時間)、セキュリティベンダーの米CheckPoint社より、Microsoft Exchange Serverの脆弱性を狙った攻撃が世界中で発生しているとして注意喚起が出されています。

- 同日時点で数百の組織が攻撃ターゲットの探索対象となり、700程度の攻撃が試みられたとしていますが、さらに同15日には同社より新たな調査結果が発表され、対象組織・攻撃数とも10倍に膨れ上がったとしています。

- 一方マイクロソフト(以下・MS)からは、同11日、オンプレミスのExchange Serverについて暫定的に脅威を緩和するツールがリリースされています。

AUS便りからの所感

- MSでは、セキュリティアップデートをまだ適用していないExchange Serverに対してこのツールを実行し、サーバーが保護されているかをガイダンスに従って確認するよう推奨していますが、脆弱性に対しての完全な緩和策となる保証はないとしています。

- アップデートの実施こそが脆弱性の根本的対策となり得ることは度々申し上げていることですが、決してそれができないとたちどころに攻撃を許してしまうような状態にはせず、今回のように何らかの回避策があるか調査し、さらにアンチウイルスやUTMにより、脆弱性を狙った攻撃を可能な限り遮断できる強固なシステム構成を随時維持することが肝要です。

TECH+ Powered by マイナビニュース

Exchange Serverへの攻撃、4日で10倍 - Check Pointデータ更新

2021/03/16 21:29　著者：後藤大地

URLをコピー

Check Point Software Technologiesは3月11日(米国時間)に「Exploits on Organizations Worldwide Grow Tenfold after Microsoft's Revelation of Four Zero-days - Check Point Software」において、Microsoft Exchange Serverに対するサイバー攻撃に関する統計情報などを伝えていた。そして、2021年3月15日(米国時間)、Check Point Software Technologiesはその内容を3月15日までのデータを加味したものへ更新した。

ITmedia NEWS

この頃、セキュリティ界隈で

Microsoft、ワンクリックの脆弱性緩和ツール公開 「Exchange Server」の脆弱性悪用続く

2021年03月17日 16時41分 公開　[鈴木聖子，ITmedia]

印刷　通知　見る　Share　B! 1

米Microsoftの電子メールサーバソフト「Exchange Server」の脆弱性を突く攻撃が拡大していることを受け、同社は3月15日、すぐには更新プログラムを適用できない組織のために、ワンクリックの緩和ツール「Microsoft Exchange On-Premises Mitigation Tool」をリリースした。

●県の川監視システム、ランサムウェアに感染…情報流出も発生か-

https://www3.nhk.or.jp/lnews/maebashi/20210319/1060008994.html
https://mainichi.jp/articles/20210321/ddl/k10/040/036000c

このニュースをザックリ言うと･･･

- 3月19日(日本時間)、群馬県より、館林土木事務所で川の堰・門等の監視システムがランサムウェアに感染したと発表されました。

- 発表によれば、感染が確認されたのは同11日で、監視情報が閲覧できない状態となった他、職員のメールアドレス、監視カメラのIPアドレスおよび水位等のデータが流出した可能性があるとのことです(県民等の個人情報の流出はないとしています)。

- 県では、出水期にあたる6月までの復旧を目指すとし、その間は県の水位雨量情報システムや職員による目視で監視するとのことです。

AUS便りからの所感

- 海外では今年2月、水処理システムの制御パネルが不正アクセスを受け、飲料水内のpH安定用の薬品濃度が瞬間的に規定値の100倍に上昇させられる事件が発生(AUS便り 2021/02/15号参照)しており、いずれも最悪の場合、実世界における人々の生活に影響を及ぼす恐れもあったという意味では共通していると言えます。

- こういったインフラ等を管理するためのネットワークとインターネットとの間は地続きにならないよう隔離し、かつマルウェアがクライアントPCを踏み台として容易に繋がり得る状態にならないよう、アンチウイルスやUTMによる防御、PCがLANに接続する際の検疫体制の確立等が重要となるでしょう。

NHK

県の川監視システムがウイルスに感染 改ざんも

03月19日　18時08分

群馬県の館林土木事務所で川のせきや門などを監視するシステムがコンピューターウイルスに感染して改ざんされ、県は原因などを調べるとともに、出水期にあたることし６月までの復旧を目指すことにしています。