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。

●京セラ複合機に情報漏えいの脆弱性…サポート連絡によるファームウェア更新を

https://news.mynavi.jp/techplus/article/20220412-2319895/
https://www.kyoceradocumentsolutions.co.jp/support/information/info_20220405.html
https://jvn.jp/vu/JVNVU94502148/

このニュースをザックリ言うと･･･

- 4月5日(日本時間)、京セラ子会社の京セラドキュメントソリューションズ社(以下・京セラDS)より、同社製の複合機に情報漏えいの脆弱性(CVE-2022-1026)が存在すると発表されました。

- 脆弱性の悪用により、機器へのログイン権限がない外部の攻撃者が、機器に登録されているアドレス帳・ユーザー名・パスワード等の情報を不正に取得可能とされています(同11日にはJPCERT/CCからも注意喚起が出されています)。

- 対象機種は、カラー・モノクロ複合機TASKalfa 55種、同ECOSYS 5種、およびプロダクションプリンターTASKalfa Pro 2機種の、計62機種となるとのことです(4月19日現在)。

- 京セラDS社では保守実施店のカスタマーエンジニアによるファームウェアの更新適用を行うとしており、その他回避策として「ファイアウォールなどで保護された環境の中での利用」「プライベートIPアドレスの使用」を挙げています。

AUS便りからの所感等

- 脆弱性は3月の時点でセキュリティスキャナー等を提供するRapid7社の技術者によって発見されていた模様で、被害を受ける情報には極めてセンシティブなものも含まれており、該当するすべての機器においてファームウェアの更新は必須となるでしょう。

- 複合機やNASあるいはいわゆるIoT機器においては、機器自身やルーターで有効になっていたUPnPによって外部からの接続が可能となるよう自動的に設定されるケース(さらには管理画面へのアクセスまで可能になっている可能性)もあり、そういった状態になっている機器を探し出す「SHODAN」「Censys」等のサーチエンジンも存在します。

- 機器自体の安全な設定やUTMの設置等によるアクセス遮断のための対策を実行した上で、依然外部からアクセス可能な状態となっていないか、第三者機関の診断や、場合によっては前述のサーチエンジンによってもポートフィルタリング状況をチェックすることが重要となるでしょう。

TECHF Powered by マイナビニュース

京セラのプリンタと複合機にデータ窃取の脆弱性、アップデートを

2022/04/12 12:21　　著者：後藤大地

JPCERTコーディネーションセンター（JPCERT/CC: Japan Computer Emergency Response Team Coordination Center）は4月11日、「JVNVU#94502148: 複数の京セラドキュメントソリューションズ製プリンタおよび複合機における認証情報の不十分な保護の脆弱性」において、複数の京セラドキュメントソリューションズ製プリンタおよび複合機に脆弱性が存在すると伝えた。

この脆弱性を悪用されると、遠隔から攻撃者によってユーザー名やパスワードといったアドレス帳内の機密データを窃取される危険性があるとされており注意が必要。

●「7-Zip」に未修正の脆弱性…回避策はヘルプファイルの削除

https://forest.watch.impress.co.jp/docs/news/1403661.html

このニュースをザックリ言うと・・・

- 4月16日(米国時間)、海外のセキュリティ研究家Kağan Çapar氏により、アーカイブ作成ソフト「7-Zip」に未修正の脆弱性(CVE-2022-29072)が存在すると発表されました。
- Çapar氏によるデモンストレーションとして、7-Zipのファイルマネージャーからヘルプを表示し、そこに細工された7zファイルをドラッグ＆ドロップすることにより、管理者権限を取得するまでの動画が公開されています。
- 脆弱性は現時点の最新バージョン21.07までに存在しており、回避策として、7-Zipのインストール先からヘルプファイル(7-zip.chm)を削除することが挙げられています。

AUS便りからの所感

- 脆弱性の悪用には、管理者権限を奪取しようとするユーザー自身がデモで挙げられているような手順をとる必要があり、「悪意のある7zファイルを開くだけで発生する」といった類のものではありません。
- 一方で、「組織のPCのユーザーがPCの管理者権限ではなく、標準ユーザー権限しか持っていない場合に、管理者権限を奪取する」ために脆弱性を悪用する可能性が挙げられ、PCに7-Zipがインストールされている場合、攻撃自体は容易なものに見受けられます。
- 7-Zipの開発者によれば、厳密にはヘルプファイルを表示するWindowsのヘルプビューアー(hh.exe)にも脆弱性が含まれており、それぞれの脆弱性の組合せによって攻撃が可能となっているとのことですが、それぞれあるいは両方に対し修正が行われるまでは、可能な限り回避策の実施を強く推奨致します。

Impress Watch

解凍・圧縮ソフト「7-Zip」に未修正の脆弱性 ～セキュリティ研究者が明らかに

ヘルプファイルの削除で緩和可能

樽井 秀人　2022年4月18日 16:15

解凍・圧縮ソフト「7-Zip」に未修正の脆弱性（CVE-2022-29072）が存在することが明らかになった。セキュリティ研究家のKağan Çaparが4月16日、その内容と攻撃を実演したビデオを「GitHub」で公開している。

それによると、v21.07（現行版）までのWindows版「7-Zip」にはファイルマネージャープロセス（7zFM.exe/7-zip.dll）のヒープオーバーフローと「Microsoft HTML ヘルプ」（HTML Help Executable Program/hh.exe）のコマンド実行機能を組み合わせることにより、管理者モードでコマンドが実行できる。「7-Zip」は［ヘルプ］－［ヘルプの表示］メニューでヘルプビューワーを開くことができるが、ここに拡張子を.7zにしたファイルをドラッグ＆ドロップすれば、特権昇格とコマンドの実行が可能になるという。

●Windows 10 21H2の提供制限が解除、アップグレードの確認を

https://forest.watch.impress.co.jp/docs/news/1403497.html
https://docs.microsoft.com/en-us/windows/release-health/status-windows-10-21h2

このニュースをザックリ言うと・・・

- 4月15日(現地時間)、マイクロソフト(以下・MS)より、Windows 10 バージョン 21H2の提供範囲を「広範な展開(broad deployment)」に設定したと発表されました。
- これまでは、21H2より前のバージョンが入っているにも拘らず、Windows Updateの設定においてバージョンアップの案内が表示されないケースもありましたが、今回の対応により基本的に全てのPCで、「Windows 10、バージョン 21H2 の機能更新プログラム」が表示され、「ダウンロードしてインストール」の実行により、バージョンアップが可能になるとのことです。
- 21H2より前のバージョンについては、20H2のサポートが5月10日リリース予定の月例セキュリティパッチで、21H1のサポートも同じく12月で終了となる予定です。

AUS便りからの所感

- Windows 10の各バージョンのサポート期間は基本的に18ヶ月間とされ、21H2の次のバージョンとしては今年後半に22H2(仮)のリリースが予定されています。
- 20H2のサポート切れ以降も引き続き21H2および21H1についてはセキュリティアップデートが提供されますが、21H2にのみ存在するような深刻な問題はもはや存在しないとみられ、通常は21H1の方を敢えて選択せず、21H2への移行を推奨致します。
- なお、同じくWindows Updateの設定画面において「Windows 11へのアップグレードの準備ができました」という案内が表示されている場合、その下に青いボタンで表示される「ダウンロードしてインストール」をクリックすると11へのアップグレードが行われてしまうことに注意し、アップグレードを希望しない場合は「今はWindows 10の使用を継続します」の方をクリックして案内を非表示にするのが良いでしょう。

Impress Watch

「Windows 10 バージョン 21H2」の提供制限は解除、広範な展開へ移行

できるだけ早いアップグレードを推奨

樽井 秀人　2022年4月18日 10:05

米Microsoftは4月15日（現地時間、以下同）、「Windows 10 バージョン 21H2」（November 2021 Update）を「広範な展開」（broad deployment）に指定したと発表した。

「バージョン 21H2」は当初提供範囲を絞り、最新のAIモデルを活用してトラブル報告をモニタリングしながら慎重にリリース範囲を拡大してきたが、報告されたトラブルの多くはおおむね解消・解決されている。「バージョン 21H2」はOSのコアを「バージョン 2004」以降と共有しており、今のところこのバージョンに固有の不具合は報告されていない。

そこで、提供範囲の絞り込みを終了し、広く提供されることになった。「バージョン 2004」以降が問題なく動作するデバイスならば、トラブルなくアップグレードできるだろう。新しい機能と最新のセキュリティ対策を導入するためにも、できるだけ早いアップグレードが推奨されている。