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。

●日本の世帯の3割が脆弱なスマートデバイス保有、6割が脆弱なルータを使用…Avastが調査

https://www.atmarkit.co.jp/ait/articles/1902/28/news041.html
https://press.avast.com/ja-jp/avast_smart_home_repor_2019_ja

このニュースをザックリ言うと・・・

- 2月26日（日本時間）、セキュリティベンダーのAvast社より、家庭で稼働するスマート機器の脆弱性に関するレポート「Avast Smart Home Report 2019」が発表されました。

- 同社のセキュリティソフトに搭載された「Wi-Fi Inspector」により、全世界で1,600万回線以上、また日本国内についても約23万回線のホームネットワークを調査したもので、以下のような結果が出ています。

◆ 日本の世帯の29%が少なくとも1台の脆弱なスマートデバイスを保有しており、ホームネットワーク全体がリスクにさらされている（世界平均：41%）

◆ 日本の家庭用ルータの57%が（古いファームウェアの脆弱性や認証設定の不備により）脆弱な状態にある（世界平均：60%）

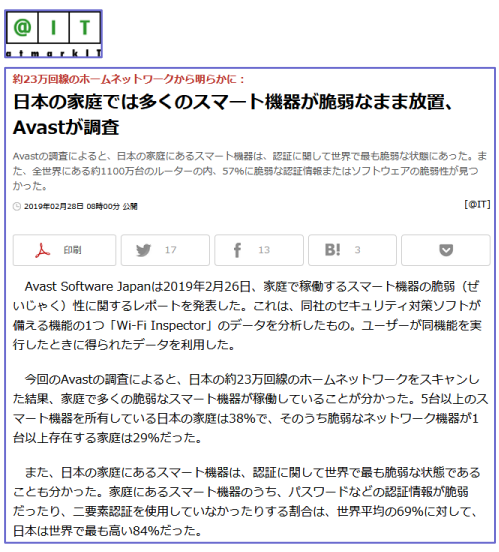
◆ ルータやネットワーク機器以外に、メディアストリーミング端末（セットトップボックス・Chromecast等）、防犯カメラ、プリンタは極めて脆弱な状態にある

AUS便りからの所感等

- 日本の家庭にあるスマート機器の84%がパスワードなどの認証情報が脆弱だったり、二要素認証を使用していなかったりしているという結果が出ており、これは世界平均の69%に比べて非常に高く、かつ世界で最も高い割合となっています。

- 総務省とNICTによる脆弱なIoT機器の調査プロジェクト「NOTICE」（AUS便り 2019/02/12号参照）は、認証設定の不備、特によく知られている簡単なパスワードを使用していないかが主な調査範囲であり、この取り組みが上記の数値の減少にどれだけ貢献するかは未知数です。

- ともあれ、最低でも機器のパスワードを独自のものに変更すること、ファームウェアを最新のバージョンにすること（これはNOTICEのページでも呼びかけられていることです）等の対策が企業であろうと家庭であろうと重要であるという認識が広がっていくことを願いたいものです。



@IT
約23万回線のホームネットワークから明らかに：
日本の家庭では多くのスマート機器が脆弱なまま放置、Avastが調査

Avastの調査によると、日本の家庭にあるスマート機器は、認証に関して世界で最も脆弱な状態にあった。また、全世界にある約1100万台のルーターの内、57%に脆弱な認証情報またはソフトウェアの脆弱性が見つかった。

2019年02月28日 08時00分 公開 [@IT]

印刷 17 13 B! 3

Avast Software Japanは2019年2月26日、家庭で稼働するスマート機器の脆弱（ぜいじゃく）性に関するレポートを発表した。これは、同社のセキュリティ対策ソフトが備える機能の1つ「Wi-Fi Inspector」のデータを分析したもの。ユーザーが同機能を実行したときに得られたデータを利用した。

今回のAvastの調査によると、日本の約23万回線のホームネットワークをスキャンした結果、家庭で多くの脆弱なスマート機器が稼働していることが分かった。5台以上のスマート機器を所有している日本の家庭は38%で、そのうち脆弱なネットワーク機器が1台以上存在する家庭は29%だった。

また、日本の家庭にあるスマート機器は、認証に関して世界で最も脆弱な状態であることも分かった。家庭にあるスマート機器のうち、パスワードなどの認証情報が脆弱だったり、二要素認証を使用していなかったりする割合は、世界平均の69%に対して、日本は世界で最も高い84%だった。

avast
Avast、日本の3世帯に1世帯が脆弱なスマートホームデバイスを所有していることを明らかに

26. 2月 2019

日本の23万回線のホームネットワークをスキャンした結果、スマートホームの新たな脆弱性を発見

- 日本の世帯の29%が少なくとも1台の脆弱なデバイスを保有、ホームネットワーク全体がリスクにさらされている (世界平均: 41%)
- 日本の家庭用ルーターの57%が脆弱な状態 (世界平均: 60%)
- ルーターやネットワーク機器以外に、メディアストリーミング端末、防犯カメラ、プリンターは極めて脆弱な状態

セキュリティソフトのベンダーであるAvastは本日、世界のスマートホームデバイスの40%がサイバー攻撃に対して脆弱な状態であることを発表しました。今回発表した「Avast Smart Home Report 2019」は、全世界で1,600万回線以上のスマートホーム・ネットワークから得られた洞察を明らかにしており、日本の家庭の38%は、5台以上のスマート機器を所有しており、こうしたデジタル世帯の29%には少なくとも1台の脆弱なネットワーク機器が存在していることが明らかになりました。脆弱なデバイスが1台でもあれば、ホームネットワーク全体のセキュリティを脅かすことになるため、今回の結果は多くの家庭がIoT (モノのインターネット) デバイスのリスクにさらされていることを物語っています。

●Windows 7にDLL読み込みの脆弱性、更新プログラムの提供はなし

https://news.mynavi.jp/article/20190228-779131/

このニュースをザックリ言うと・・・

- 2月28日（日本時間）、IPAより、脆弱性ポータルサイト「JVN」において、Windows 7の標準ライブラリ（DLLファイル）の読み出しに関する、いわゆる「DLLインジェクション攻撃」についての情報が出されています。

- プログラムの実行時、システムにインストールされているDLLと同じ名前のDLLがプログラムと同じフォルダにある場合、そちらを優先的に読み込む場合があり、細工したDLLにより、不正なコードを実行される可能性があるとされています。

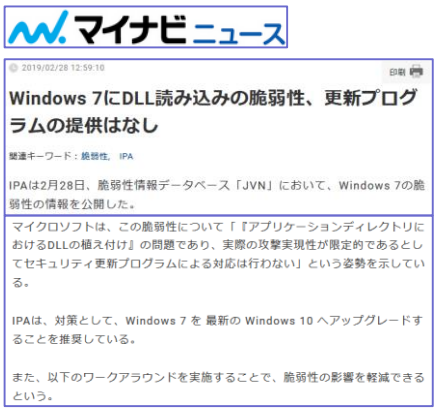
- マイクロソフトでは、Windows 10 Creators Update(1703)以降でこの問題を緩和する機能を採用しましたが、Windows 7での修正を行う予定はないとしており、Windows 10へのアップグレード等を推奨しています。

AUS便りからの所感等

- このDLLインジェクションの問題は今回初めて話題となったものではなく、2017年頃にJVN等において注意喚起が出されていたもので、例えば「ダウンロード」フォルダに保存されたインストーラーを実行しようとするケースを狙い、そこに不正なDLLファイルを置くことが攻撃の一例として挙げられていました。

- Windows 7は来年1月に主なサポートの終了が予定されていること、またOSの動作に影響する変更を伴うことから、採用されなかったと考えられます。

- Windows 10は他にも7に比べ様々なセキュリティ機能が取り入れられていますので、可能な限りサポート終了を待つまでもなく移行していくことは大事とは言える一方、ダウンロードフォルダ（およびデスクトップ）が煩雑にならないよう普段から整理しておくことも不正なDLLファイルが紛れ込むことがないようにする意味では大切です。



●Chromeのゼロデイ脆弱性が修正…PDFリーダーとは別の問題

https://www.itmedia.co.jp/enterprise/articles/1903/07/news078.html

このニュースをザックリ言うと・・・

- 3月1日（米国時間）、Google Chromeの最新バージョン72.0.3626.121がリリースされ、危険度が高いとされる脆弱性1点が修正されました。

- 後日、リリースの時点で悪用が確認されていたゼロデイ脆弱性であることが発表されており、細工されたWebページを開くことにより、PCをリモートから乗っ取られる可能性もあるとされています。

- なお、ChromeのPDFリーダー機能で発見されていた脆弱性（AUS便り 2019/03/04号参照）とは別の脆弱性とのことです。

AUS便りからの所感等

- 脆弱性が存在したのはFileReaderというWeb機能の一つで、ユーザ側が指定したPC上のローカルファイルをWebページ上で処理するために用いられますが、今回の脆弱性は、例えばWebページ側が指定したローカルファイルを勝手に読み込まれてしまうといったものではないと思われます。

- Chromeは通常自動更新が有効になっているため、現時点では多くのPCで最新バージョンにアップデートしているはずですが、念のためバージョン情報を確認（確認の際にも自動更新がはたらき、古いバージョンからアップデートされます）すること、また自動更新はできるかぎり無効にはしないことが重要です。