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。

●任天堂、10年以上前に販売したWi-Fi機器の使用中止呼び掛け…暗号化通信解読の恐れ等

https://nlab.itmedia.co.jp/nl/articles/2207/20/news122.html
https://www.nintendo.co.jp/support/information/2022/0720.html

このニュースをザックリ言うと･･･

- 7月20日(日本時間)、任天堂より、同社がDS・Wiシリーズ用に販売していた古いネットワーク機器について注意喚起が出されています。
- 対象となる機器は、2005年11月発売の「ニンテンドーWi-Fi USBコネクタ(NTR-010)」および2008年9月発売の「ニンテンドーWi-Fiネットワークアダプタ(WAP-001)」です。
- いずれもWi-Fi暗号化方式としてはWEPにしか対応しておらず暗号化通信の解読の恐れがあり、また後者は他にも機器の乗っ取りが可能な脆弱性があるとして、使用を中止し、市販のネットワーク機器等に切り替えるよう呼び掛けられています。

AUS便りからの所感等

- 各機器ともすでに発売から10年以上が経過しており、これらやDS発売(2004年12月)の時点でWEPのセキュリティ上の問題点の解決等を目的とした後継規格となるWPA(2002年)やWPA2(2004年)が発表されていたものの、対応していないという状況でした。
- WPA2等においても後年プロトコルに脆弱性が指摘され、その時点でサポートが続いている機器やOSではアップデートによって修正が行われていますが、前述の機器のように販売が終了し、ファームウェアアップデートが提供されないものは、使用の継続により、未修正の脆弱性を悪用される可能性が発生します。
- 今回のケースを単にゲーム機の周辺機器でのものと捉えることなく、組織で使用している全てのネットワーク機器についてサポートが切れたものが存在しないか把握し、速やかに交換できるような管理体制を整えることが重要です。

ITmedia NEWS

任天堂が自社のWi-Fi機器2種の使用中止を呼びかけ 不正アクセスやウイルス感染のおそれ

市販機器への切り替えを推奨しています。

［コンタケ, ねとらぼ］

任天堂が7月22日、「ニンテンドーWi-Fi USBコネクタ」と「ニンテンドーWi-Fiネットワークアダプタ」の使用中止を呼びかけました。使用を継続すると、外部からの不正アクセスや、コンピュータウイルス感染などのおそれがあるとしています。

●Twitterアカウント情報540万人分流出、闇サイトで販売か

https://news.mynavi.jp/techplus/article/20220725-2407330/
https://coinpost.jp/?p=370293
https://restoreprivacy.com/twitter-vulnerability-exposes-5-million-accounts/

このニュースをザックリ言うと･･･

- 7月21日(米国時間)、セキュリティ情報サイト「Restore Privacy」より、Twitterユーザー540万人分のアカウント情報が流出した可能性があると発表されました。

- Twitterアカウントの電話番号・メールアドレスが非公開であっても取得可能な脆弱性が1月にバグ報奨金プラットフォーム「HackerOne」で報告(現在は修正)されており、これを悪用して奪取したとみられる情報がアンダーグラウンドのハッキングフォーラムで販売されていたとされ、データの対価として3万ドルを要求していたとのことです。

- このハッキングフォーラムにおいては、7月4日、中国の国民約10億人分の個人情報を含むデータを2,700万円相当のビットコインで販売するとした人物も現れています。

AUS便りからの所感

- 今回流出した情報には、パスワードをはじめ、各アカウントへのログインや権限の利用が直接可能になる情報は含まれていなかった模様ですが、情報の購入者等からメールアドレスや電話番号に対しフィッシングメール・SMSが送信される可能性があるとして注意が呼び掛けられています。

- 今後Twitter公式等から、対象となったアカウントへ何らかの連絡があるか、あるいはユーザー側が確認する手段が提供されるか等も注目されますが、いずれにせよ情報を登録していたユーザーについては今後フィッシングにさらに警戒するに越したことはないでしょう。

Twitter、540万のアカウント情報が窃取された可能性浮上-闇サイトで販売

2022/07/25 09:46　著者：後藤大地

Twitter　情報漏えい　サイバーセキュリティ　サイバー攻撃　脆弱性

Restore Privacyは7月21日(米国時間)、「Verified Twitter Vulnerability Exposes Data from 5.4 Million Accounts | RestorePrivacy」において、540万人分のTwitterアカウント情報が流出したと伝えた。2022年1月に発覚したTwitterの脆弱性が悪用され、サイバー犯罪者によって540万人のユーザーのアカウントデータが窃取された可能性が浮上した。

今年1月、バグ報奨金プラットフォーム「HackerOne」のユーザーであるzhirinovskiy氏によって、プライバシー設定で非表示にしてもTwitterアカウントに関連する電話番号やメールアドレスが取得できてしまうという脆弱性が報告されていた。このバグはTwitterのAndroidクライアントで使われている認証プロセスで発生していた。

●Emotet感染拡大、勢い続く…JPCERT/CC 4～6月脅威情報まとめ

https://news.mynavi.jp/techplus/article/20220715-2399089/
https://www.jpcert.or.jp/newsflash/2022071201.html

このニュースをザックリ言うと･･･

- 7月12日(日本時間)、JPCERT/CCより、2022年4月～6月にかけて確認された影響範囲の広い脆弱性情報・脅威情報等のまとめが発表されました。

- 今年2月にも感染が急速に拡大したマルウェア「Emotet」については、4月下旬以降、拡張子が「lnk」のショートカットファイル(およびそれを含むパスワード付きZIPファイル)を添付したメールによる拡散がみられています(AUS便り 2022/05/10号参照)。

- この他、6月15日をもって(Windows10での)IE11のサポートが終了したことも取り上げられています(同2022/06/14号参照)。

AUS便りからの所感

- まとめで言及されているものとしては、この他にSpring Frameworkの脆弱性(同2022/04/05号参照)等があります。

- ユーザーにおいても管理者においても、JPCERT/CCやIPA等の各セキュリティ関連組織が随時リリースしている注意喚起や今回のようなまとめ情報の収集を日々行うとともに、自組織で使用しているプロダクト等で更新の必要があるものについてすぐにアップデート等の対応ができる体制を整えることが肝要です。

JPCERT/CCが4月～6月の脆弱性・脅威を振り返るレポート公開、Emotet感染止まらず

2022/07/15 10:27　著者：後藤大地

脆弱性　JPCERT/CC　サイバー攻撃　サイバーセキュリティ　マルウェア

JPCERTコーディネーションセンター(JPCERT/CC: Japan Computer Emergency Response Team Coordination Center)は7月12日、2022年4月から6月にかけて確認された影響範囲の広い脆弱性情報や脅威情報を振り返るレポートを公開した。

- 2022年4月から6月を振り返って

このレポートは、最新のトレンドを考慮した組織のセキュリティ対策の強化につなげることを目的として作成されたもの。2022年4月から6月にかけて特に目立ったサイバー攻撃活動やJPCERT/CCの取り組みなどがまとめられている。