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。

●バッファローに続きNEC Atermシリーズでも脆弱点発表、最新ファームウェアへの更新または回避策実施を

https://ascii.jp/elem/000/004/387/4387155/
https://jvn.jp/jp/JVN89339669/
https://jpn.nec.com/security-info/secinfo/nv26-001.html

このニュースをザックリ言うと・・・

- 3月26日(日本時間)、NEC社より、同社製「Aterm」シリーズのWi-Fiルーター・中継器等に複数の脆弱点が存在するとして注意喚起が出されています。
- 脆弱点は計5件が存在し、機器と同一LAN上にいる攻撃者により、設定情報の奪取や改変、機器上でファイルの改ざんや任意のコード実行、および非公開のバックドア機能の有効化が可能とされています。
- 4月3日にはIPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」からも注意喚起が出されています。
- 一部機器においては最新版のファームウェア(2025年1月までにリリース済みの模様です)への更新で対策されており、その他の機器については回避策として管理者パスワードおよびWi-Fi接続用の暗号化キーを複雑なものに設定するよう呼び掛けられています。

AUS便りからの所感等

- 3月23日にはバッファロー社からも同社製ネットワーク機器において複数の脆弱点とセキュリティアップデートのリリース(一部機種除く)が発表されています(「AUS便り 2026/04/03号」参照)。
- 脆弱点は外部ネットワーク上から直接悪用は不可能とされますが、一旦同一LAN上に侵入した上で攻撃を行われるシナリオは当然考えられます。
- ファームウェアの自動更新が有効な機種であれば既に対策済みとみられますが、一部手動での更新確認が必要とされる機種や、サポート期間中ながらファームウェア側では対策されていない機種(今後アップデートがリリースされる可能性もあります)、またNEC「Atermにおける複数の脆弱性」のページには対象製品として掲載されず、同ページ「対処方法」からリンクされているページには掲載されている機種もありますので、組織内で利用している機種について掲載されているか十分に確認した上で適切な対応をとり、サポート終了済みの機器についても確実にリプレースを行うこと、また強固なパスワードの設定は脆弱性の有無に拘わらず実施することが肝要です。

ASCII.jp

NEC「Aterm」シリーズに複数の脆弱性　アップデートまたは買い換えを推奨

2026年04月03日 17時30分更新　　文● スミーレ（@sumire_kon）

Japan Vulnerability Notes（JVN）は4月3日、日本電気（NEC）製の複数のWi-Fiルーターに関する脆弱性情報を公開した。

脆弱性の概要と想定される影響は、それぞれ以下のとおり。

●脆弱性の概要

・権限チェックの欠如（CVE-2026-4309）
・パストラバーサル（CVE-2026-4619）
・OSコマンドインジェクション（CVE-2026-4620／CVE-2026-4622）
・セキュリティ上問題のある隠し機能（CVE-2026-4621）

●想定される影響（一例）

・装置固有の情報を取得され、結果として設定を変更される（CVE-2026-4309）
・任意のファイルを上書きされる（CVE-2026-4619）
・任意のOSコマンドを実行される（CVE-2026-4620／CVE-2026-4622）
・telnetサービスを有効化される（CVE-2026-4621）

● JavaScript HTTPクライアントライブラリ「axios」、一時有害なバージョン配布…インストールでマルウェア感染の恐れ

https://blog.flatt.tech/entry/axios_compromise
https://github.com/axios/axios/issues/10604

このニュースをザックリ言うと･･･

- 3月31日(日本時間)、JavaScript製HTTPクライアントライブラリー「axios」において、いわゆるサプライチェーン攻撃により、一時マルウェアを含む有害なバージョンが配布されていたとして、ブログ・SNS等で注意喚起が出されています。

- axios開発者のnpm(パッケージ管理・配布システム)のアカウントが攻撃者に乗っ取られ、3月31日9:21～12:15頃の間にバージョン1.14.1および0.30.4がリリースされており、インストールしたサーバーがRAT(管理者権限を持ち外部からの遠隔操作を受けるトロイの木馬の一種)に感染する恐れがあったとされています。

- 有害なバージョンは現在npm等から削除されており、バージョン1.14.0以前および後日リリースされた1.15.0には問題はないとされています。

AUS便りからの所感

GMO Flatt Security Blog

- axiosの有害なバージョンはそれ自体のコードに改変はなく、依存ライブラリーとして追加された「plain-crypto-js」のインストール時にRATをダウンロードする仕掛けがあったことが、GMO Flatt Security社のブログ等で明らかになっています。

- 前述したブログでは、プログラム自体がaxiosをインポートしていなくても他のライブラリーからインポートされていることもあるとし、悪意のあるプログラムファイル等がインストールされていないか等の各種確認を呼び掛けるとともに、npmにおいてリリースから数日経過したバージョンのみインストールするよう設定すること等を推奨しています。

- 依存するライブラリーのインストール時、あるいはWebページから外部CDN上のスクリプトを読み込む際、最新バージョンを読み込む設定で、意図せず不審なバージョンを読み込む可能性があることから、信頼のおけるバージョンに固定すること、さらにはスクリプトが改ざんされていないか検出するSubresource Integrity機構等を活用することは有用と言えます(一方で後に脆弱性が発見されたバージョンを使い続けるリスクもあり、随時バージョンを更新すべきか確認することも必要です)。

●JPCERT/CC配布のEmotetチェックツール配布終了…Emotet沈静化およびツール自体の脆弱性のため

https://forest.watch.impress.co.jp/docs/news/2100704.html
https://www.jpcert.or.jp/press/2026/PR20260410.html
https://jvn.jp/jp/JVN00263243/
https://github.com/JPCERTCC/EmoCheck

このニュースをザックリ言うと･･･

- 4月10日(日本時間)、JPCERT/CCより、マルウェア「Emotet」検出ツール「EmoCheck」の配布を終了するとともに、同ツールの使用を停止するよう呼び掛けられています。

- 同日にJVNより、EmoCheckにDLL読込に関する脆弱性が存在することが発表されており、これを呼び掛けの理由の一つとしています。

- Emotetはオンラインバンキングのアカウント情報を奪取する攻撃を行うマルウェアで、2018～2019年に特に被害が拡大し、その後もこれを用いた攻撃は度々確認されていた模様ですが、JPCERT/CCでは2023年4月以降、Emotetの活動を確認しておらず、脅威がなくなったとしています。

AUS便りからの所感

Impress Watch

- DLL読込の脆弱性は、プログラムファイルと同じフォルダー上に不正なDLLファイルが置かれている場合、実行時にこのDLLファイルを読み込む可能性があるというもので、脆弱性のあるインストーラーやプログラムファイルをWindowsの「ダウンロード」フォルダーやデスクトップ上から実行するケースを狙い、事前に悪意のあるDLLファイルを配置する攻撃等が指摘され、過去非常に多くのWindowsアプリケーションで報告・対策されています。

- 当該脆弱性の回避策として、インストーラーやプログラムファイルのダウンロード～実行は「ダウンロード」「デスクトップ」フォルダーとは別のフォルダーで行うことが挙げられます。

- 一方で、開発元から更新停止・開発終了が宣言されたソフトウェアを使い続けることも未修正の脆弱点を突かれる恐れがあり、現在利用しているソフトウェアの更新状況等を随時確認し、開発終了したソフトウェアを使い続けることは一般に避けるべきでしょう。