— AUS（アルテミス・ユーザ・サポート）便り 2024/4/10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。

●NEC製のWi-Fiルーター59製品に脆弱性、回避策適用やリプレースを

https://internet.watch.impress.co.jp/docs/news/1582716.html
https://jvn.jp/jp/JVN82074338/index.html
https://jpn.nec.com/security-info/secinfo/nv24-001.html
https://aterm.jp/support/tech/2024/0227.html

このニュースをザックリ言うと･･･

- 4月5日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、NECプラットフォームズ社(以下・同社)提供のWi-Fiルーター「Aterm」シリーズに脆弱性が存在するとして注意喚起が出されています。
- 脆弱性の悪用により、機器のtelnetポート・UPnP等から不正なコードを実行され、機器を乗っ取られる等の可能性があるとされています。
- 脆弱性が確認されたのは59製品にのぼり、一部サポートが終了している機器もあります。
- 同社ではファームウェアの更新は提供しておらず、回避策として「Web管理画面のパスワードとWi-Fi暗号化キーを初期の値から変更すること」「UPnPの無効化」を挙げ、サポート終了機器については交換することを呼び掛けています。

AUS便りからの所感等

- telnetポート(TCPポート23番)は内部ネットワーク側からのみアクセス可能ですが、攻撃者が社内LANに侵入した場合に機器にハードコードされたアカウント情報でログインされる等の恐れがある上、設定で無効化できない場合がある模様です。
- 回避策のうち「Web管理画面のパスワードとWi-Fi暗号化キーの変更」は、脆弱性の有無に拘わらず、あらゆるネットワーク機器においてセットアップ時に必ず行うべきです。
- 対象機器には発売から10～15年近く経っているものもあり、古い機器は故障するまで使い続けられたり、ファームウェア更新を含めた管理が行き届いていない可能性もありますので、家庭・企業に拘わらず、使用されている各ネットワーク機器について機種を含め把握・管理し、機器交換についても計画的に行えるような体制を整えることが肝要です。

Impress Watch

「Aterm」シリーズのWi-Fiルーターなど59製品に複数の脆弱性。対策や買い替えの検討を

山田 貞幸　2024年4月9日 10:25

Aterm WG1800HP4

日本電気株式会社（NEC）は、「Aterm」シリーズのWi-Fiルーターやルーター59製品に複数の脆弱性があるとして情報を公開した。JVN（Japan Vulnerability Notes）でも、本件に関する情報を公開している。

対象となる59製品のうち、次の49製品については、脆弱性により起こる3つの現象と、その対策を、NECが提示している（以下の一覧における、製品型番の後ろのカッコ内が現象の番号。具体的な内容と対策は後述）。

●現象1 telnet経由で任意のコマンドが実行される
悪意ある第三者が製品にアクセスした場合、telnet経由で任意のコマンドが実行される可能性がある。対策としては、管理画面へのログインパスワードや、Wi-Fi接続のパスワードを、初期値でなく堅牢なものに変更する。

●現象2 UPnP経由で任意のコードが実行される
悪意ある第三者が製品にアクセスした場合、UPnP経由で任意のコマンドが実行される可能性がある。対策としては、製品のUPnPを無効化する。クイック設定Webの詳細モードで「基本設定」を開き、「UPnP設定」を「使用しない」に変更し、設定を保存する。

●現象3 任意のコマンドが実行される
悪意ある第三者が製品にアクセスした場合、任意のコマンドが実行されたり、装置名などの装置情報が読み取られる可能性がある。対策としては1と同じく、対策としては、管理画面へのログインパスワードや、Wi-Fi接続のパスワードを、初期値でなく堅牢なものに変更する。

● Bing検索でトップに偽サイトが…悪意のある広告に注意

https://togetter.com/li/2339709
https://news.mynavi.jp/techplus/article/20240407-2921778/

このニュースをザックリ言うと・・・

- 3月27日(日本時間)、X(旧Twitter)において、Bingで「アマゾン」と検索した結果のトップにamazonを騙る偽サイトが表示されるというポストがあり、話題になっていました。

- 表示されているリンクには「amazon.co.jp」と表示されていますが、実際には別のドメイン名のもので、アクセスにより偽のセキュリティ警告が表示される、いわゆる「サポート詐欺」のサイトとなっているとのことです。

- 4月10日時点では同様の検索でサポート詐欺のサイトの表示は確認されていませんが、SNS上で問題などが報告されているECサイト「Temu」が広告として表示される等しています。

AUS便りからの所感

- Bingでは他にもVPNソフトウェア「NordVPN」の偽サイトが広告に表示される事例がセキュリティベンダーのMalwarebytes社によって報告されています。

- 偽のセキュリティ警告でとられる手口の例については、IPAが公開している体験サイト(AUS便り 2023/12/20号参照)で事前に把握することを推奨致します。

- BingのみならずGoogleでも、有名なソフトウェアの検索時において偽の公式サイトが広告に表示される事例(同2023/10/25号参照)、さらにはSNSや個人のWebサイトで貼られている広告でも同様に危険なものが散見され、アンチウイルス・UTMによるアンチフィッシング機能に加え、Webブラウザーに広告ブロック拡張を導入することもセキュリティ対策として検討すべき情勢といえます。

● Microsoft・Adobeより月例のセキュリティアップデート、来週はOracleからも四半期定例アップデート予定

https://forest.watch.impress.co.jp/docs/news/1583046.html
https://msrc.microsoft.com/blog/2024/04/202404-security-update/
https://forest.watch.impress.co.jp/docs/news/1583058.html

このニュースをザックリ言うと・・・

- 4月10日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5036892(ビルド 19045.4291)および11 23H2 KB5036893(ビルド 22631.3447)となります。

- 同日にはAdobe社からもPhotoshop等に対するセキュリティアップデートがリリースされています。

AUS便りからの所感

- MSのセキュリティアップデートについては、既に悪用が確認されている、いわゆる「ゼロデイ」の脆弱性も含まれており、可能な限り速やかに適用が推奨されます。

- 翌週4月17日にはOracleからもJava等に対する四半期の定例アップデートが予定されています。

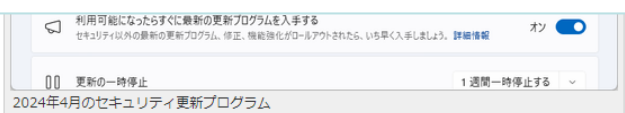
- 今後発生し得る新たな攻撃に備え、確実にアップデートを適用すること、それまでに発生する攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。

Impress Watch

2024年4月の「Windows Update」がリリース、Windows 11には賢い「スナップ レイアウト」も

CVE番号ベースで147件の脆弱性が新たに対処、緊急の脆弱性は3件

樽井 秀人　2024年4月10日 09:30



米Microsoftは4月9日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで147件の脆弱性が新たに対処されている。