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。

## ●「Aterm WG2600HS」など複数のNEC製のWi-Fiルーターに脆弱性、最新版へのアップデートを

https://internet.watch.impress.co.jp/docs/news/1236069.html

### このニュースをザックリ言うと・・・

- 2月19日(日本時間)、NECより、同社製のWi-Fiルーター「Aterm」シリーズの一部に脆弱性が発見されたとして注意喚起が出されています。
- 脆弱性の影響を受けるのはAterm WG2600HS、WF1200CRおよびWG1200CRで、管理画面等にログイン可能な攻撃者により、ルーターのOS上で任意のコマンドを実行される可能性があるとされています(WG2600HSにはクロスサイトスクリプティングの脆弱性もあり)。
- 脆弱性を対策したファームウェアもリリースされており、アップデートが強く推奨されています。

### AUS便りからの所感等

- 脆弱性が確認されたのは全て据え置き型のルーターで、モバイルルーターは対象外です。
- 今回これら以外の据え置き型機種に脆弱性があるかどうかは発表されていませんが、Atermシリーズは原則完売から7年でサポート終了となる(https://internet.watch.impress.co.jp/docs/special/1114330.html )とのことで、機種によっては脆弱性があったとしても修正されない可能性があります。
- 他社機種も含め、社内にある全てのネットワーク機器について、ファームウェア等のアップデート方法、アップデートのリリース情報、機器自体がアップデートのリリースを知らせてくれる機能を把握し、確実に最新の状態に保つ体制、そしてサポートが終了した、あるいは終了したと見られる機種を新しいものと交換する体制を整えることが重要です。

INTERNET Watch

「Aterm WG2600HS」など複数のNEC製のWi-Fiルーターに脆弱性、最新版へのアップデートを

磯谷 智仁　2020年2月19日 15:12


日本電気株式会社（NEC）が提供するAtermシリーズの複数の無線LANルーターに脆弱性が存在するとして、同社および脆弱性対策情報ポータルサイト「JVN（Japan Vulnerability Notes）」が情報を公開した。

## ●500個ものChrome拡張機能が個人情報を盗んでいたことが判明、被害者は170万人を超える

https://gigazine.net/news/20200217-chrome-extension-malware-malvertising/

### このニュースをザックリ言うと・・・

- 2月13日(現地時間)、セキュリティ企業Duo Security社の研究者より、Chromeブラウザーにおいて約500個の不正な拡張機能(アドオン)を確認し、Google公式のChromeウェブストアから削除されたと発表されました。

- 発表によれば、同社のChrome拡張機能安全評価ツールにより、70個の拡張機能がサイバー攻撃命令を送信する指令サーバーにアクセスしていたことを発見、Googleと連携し、さらに470個の拡張機能が同様の挙動を示していたことを確認したとのことです。

- これらの拡張機能は広告表示を装って指令サーバーと通信し、個人情報を盗み出していたとされ、インストールしていたユーザーは170万人を超えているとのことです。


GIGAZINE

2020年02月17日 12時00分 セキュリティ

500個ものChrome拡張機能が個人情報を盗んでいたことが判明、被害者は170万人を超える

「Chromeウェブストア」から拡張機能をインストールすると、ブラウジングを快適にしてくれる機能を簡単にChromeに導入可能ですが、中には便利なツールを装って不正な動作をする拡張機能も存在しており、過去には200個もの拡張機能が一斉に削除されたこともあります。今回新たに、合計500個以上のChrome拡張機能が不正に個人情報を入手していたことが、セキュリティ研究者らの調べにより発覚しました。

Security researchers partner with Chrome to take down browser extension fraud network affecting millions of users. | Duo Security
https://duo.com/labs/research/crxcavator-malvertising-2020

500 Chrome Extensions Caught Stealing Private Data of 1.7 Million Users

### AUS便りからの所感

- ブラウザーの拡張機能は、その仕様上ブラウザのほぼ全ての機能を操作し、あるいはデータを読み取ることが可能となっており、インストール時には、どの範囲の操作やデータの読み取りを要求するかの警告が表示されます(アップデート時、要求する権限の範囲が広まった場合にも警告が出ます)。

- スマートフォンアプリでも言えることですが、インストールの際にはウェブストアのレビューやSNS等ネット上の情報を十分確認し、必要最低限のもののみインストールするよう心がけましょう。

## ●日本郵便に不正アクセス、約4,000通のメール送信…「原因や被害状況など調査中」

https://www.itmedia.co.jp/news/articles/2002/17/news086.html
https://www.post.japanpost.jp/notification/productinformation/2020/0214_02.html

### このニュースをザックリ言うと・・・

- 2月14日(日本時間)、日本郵便より、同社のメールアカウントが不正アクセスを受け、外部への意図しないメール送信に悪用されたと発表されました。

- 被害を受けたのは同社が保有する「@jp-international.jp」ドメインのアカウントで、2月6日～7日にかけて約4,000通のメールが送信されたとのことです。

- 同社では7日に事態を把握し、当該アカウントのパスワード変更および外部への接続遮断を行っており、攻撃手法や原因、被害の詳細等は現在調査中とのことです。

### AUS便りからの所感

- 2月7日に長岡技術科学大学から発表された同様の不正アクセスでは、メールボックスに保存されていたメールを読み取られ、個人情報を閲覧された可能性が示唆されています(AUS便り 2020/2/17号参照)が、今回のケースで同様の問題が発生していたかはまだ不明です。

- 外部からメールサーバーを直接攻撃された可能性、クライアントPCを踏み台にした可能性、いずれにおいても、不審な外部へのメール送信を食い止められるよう、とり得る対策を可能な限りとっていくことが推奨され、前者については サーバー側での設定(送信量の制限、不審なログイン試行の遮断等)、後者については アンチウイルス・UTMによる対策等が考えられます。


ITmedia NEWS

日本郵便に不正アクセス、4000通のメールを誤送信　「原因や被害状況など調査中」

2020年02月17日 14時32分 公開 [ITmedia]

印刷 見る Share B! 21

日本郵便は2月14日、同社のメールアカウントが第三者から不正アクセスを受け、約4000通の意図しないメールが送信されたと発表した。メールは6～7日にかけて送信されたという。同社は7日に事態を把握し、原因や被害状況など詳細を調査している。

お知らせ
当社保有メールアカウントからの意図しないメール送信について
2020年2月14日

日本郵便による発表

不正アクセスを受けたのは、同社が保有するメールアドレスのドメイン「@jp-international.jp」。日本郵便は対策として、メールアカウントのログインパスワードを変更し、外部との接続も遮断。専門家を交えて不正アクセスの手法や原因、被害状況について調査中だとしている。