セキュリティレポート

2023.7

YOU DESERVE THE BEST SECURITY

エレコム製無線LANルーターに複数の脆弱性

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は7月11日、
エレコム製無線 LAN ルーターにおける複数の脆弱性について「Japan Vulnerability Notes（JVN）」で発表しました。

脆弱性主な影響・・・

・ウェブ管理画面におけるコマンドインジェクション（CVE-2023-37566、CVE-2023-37568）
↓
ログイン可能な第三者によって、ウェブ管理画面に対して細工されたリクエストを送信され、任意のコマンドを実行される。

・ウェブ管理画面の特定ポート番号におけるコマンドインジェクション（CVE-2023-37567）
↓
遠隔の第三者によって、ウェブ管理画面の特定のポート番号に対して細工されたリクエストを送信され、任意のコマンドを実行される

CHECK POINT

速やかなアップデート

現在利用されているWi-Fiルーターが下記の方式に一致するのであれば、

速やかにアップデートを実施してください。

機種型式

・CVE-2023-37566
WRC-1167GHBK3-A v1.24 およびそれ以前のバージョン
WRC-1167FEBK-A v1.18 およびそれ以前のバージョン

・CVE-2023-37567
WRC-1167GHBK3-A v1.24 およびそれ以前のバージョン

・CVE-2023-37568
WRC-1167GHBK-S v1.03 およびそれ以前のバージョン
WRC-1167GEBK-S v1.03 およびそれ以前のバージョン

CHECK POINT

こんなWi-Fi使っていませんか？

★ 氏名や社名の語呂合わせなど推測しやすい情報をSSIDや暗号化キーに使っている

★ 住所の番地や電話番号など公になっている情報をSSIDや暗号化キーに設定している

★ 同じ数字の組み合わせを暗証番号やパスワードなど複数の場所で使い回している

★ 古いルーターを初期設定のまま使い続けている

★ 暗号化が設定されていない（パスワードを入力しなくてもWi-Fiにつながる）

★ 解読方法が広く知られている暗号化規格のWEPを利用している

★ Wi-Fiルーターの管理画面のパスワードが「admin」や「password」のまま

★ 長らくファームウェアの更新をした記憶がない

★ Wi-Fiルーターの脆弱性に関する情報をチェックしていない

★ リスクを考慮せず誰もがつながるWi-Fiを公開している/使っている

★ 不特定多数の利用者がつなぐWi-Fiで端末間通信を禁止していない

CHECK POINT

会社内で意識する事・出来る事

- SSIDを利用者が想定しにくいものに変更する
- 暗号化キーを複雑な文字列に変更する
- 暗号化を必ず有効にする
- WPA3、なければWPA2などの最新の安全な暗号化方式を使う
- Wi-Fiルーターの管理者画面のパスワードを複雑なものに変更する
- 定期的にファームウェアの更新を実施する
- 自動的にファームウェアを更新できる最新機種に交換する
- 管理画面のパスワードを複雑なものに変更する
- メーカーのサポートページやセキュリティ情報を定期的に確認する
- サポート切れで更新が提供されない場合は利用を中止し買い換えるが充実している最新のWi-Fiルーターに買い換える
- 端末間通信を禁止する
- フリーWi-Fi利用時の注意点やリスクを利用者に伝える
- 利便性は低下するが暗号化設定や認証の仕組みを検討する
- 利用者の安全を確保できない場合はフリーWi-Fiの提供中止も検討する
- フリーWi-Fiを利用する場合も暗号化の有無や端末間通信の禁止を確認する

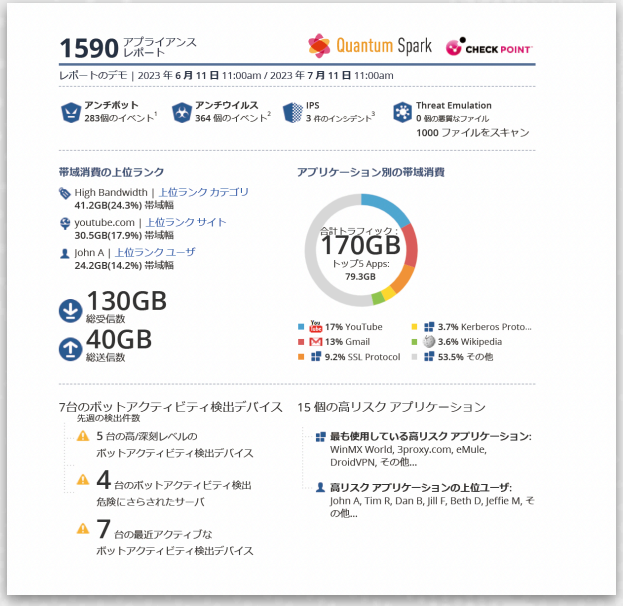
大企業向けに開発した最高レベルセキュリティ機能を中小企業へ

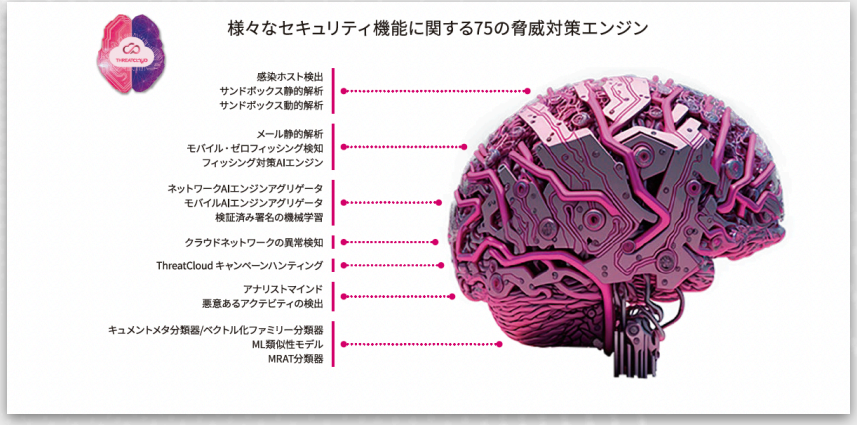
最先端の最高レベルセキュリティが１台で実現できるから
コストを抑えたトータル・セキュリティ・ソリューションが可能です

中小企業向けUTM

インターネット上に存在する様々脅威に対し、多段階の防御策を実現することができるネットワーク製品です。
社内ネットワークの手前で遮断することにより、安全なネットワーク環境でご利用いただけます。

Quantum spark





レポートも見やすく運用も容易！

導入から運用まで、システム担当者がいない中小企業様でも安心して管理・運用が可能な総合脅威対策機器です。

デジタルカタログは
https://cp-smb.com/catalog/

CHECK POINT