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。

●エレコム製のWi-Fiルーター6製品に脆弱性、ファームウェアアップデートを

https://pc.watch.impress.co.jp/docs/news/1613104.html
https://www.elecom.co.jp/news/security/20240730-01/
https://jvn.jp/jp/JVN06672778/

このニュースをザックリ言うと･･･

- 7月30日(日本時間)、エレコム社より、同社提供のWi-Fiルーター6機種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、機器上で任意のコマンドを実行される可能性、および管理画面へログイン可能なユーザーにクロスサイトリクエストフォージェリ(CSRF)を実行させられる可能性があるとしています。
- 同社では脆弱性が確認された各機器に対しファームウェアのアップデートを提供しています。
- IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」からも同日に脆弱性の注意喚起が出されており、CSRFにより、ログインIDやパスワードを攻撃者が指定した内容に変更される恐れがあるとしています。

AUS便りからの所感等

- ファームウェアは既定で自動更新が行われるとのことですが、実際に最新のバージョンとなっているか管理画面で確認することを推奨致します。
- 特にネットワーク機器の管理画面ではログインした後に明示的にログアウトする機構がなく、ブラウザーを閉じるまでログインしたままの状態となるケースもあるところから、CSRFによる不正行為のターゲットとなりやすいため、管理画面へのログインは別途「シークレットウィンドウ」を開いて行うよう心掛けましょう。
- 使用しているネットワーク機器のメーカーからのセキュリティに関する情報について、特に組織の管理者は常時、また家庭で使用している場合でも適宜巡回して確認すること、またサポートが終了した機器に脆弱性が見つかり、メーカーから発表はあってもセキュリティアップデートは提供されないケースもあり、これに備え機器のリプレースを確実に行う体制の確立が肝要です。

Impress Watch

エレコムの無線LANルーターに脆弱性。ファームウェア更新を呼びかけ

浅井 淳志　2024年8月1日 15:38

ポスト　リスト　シェア　はてブ　note　LinkedIn

WRC-2533GS2-B

一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)と独立行政法人情報処理推進機構(IPA)が共同で運営しているJVNは30日、エレコム製の無線LANルーターに複数の脆弱性があるとして、注意喚起を促した。

脆弱性を悪用されると、第三者が対象製品にログインし、細工されたファイルやリクエストを送信して任意のOSコマンドを実行する恐れがある(CVE-2024-34021、39607)。

ELECOM LIFESTYLE INNOVATION

EL40-081
2024.07.30

セキュリティ情報

無線LANルーターのセキュリティ向上のための
ファームウェアアップデート実施のお知らせ

対象製品と対処方法

脆弱性内容：
①悪意のある第三者にログインされると、任意のコマンドを実行される可能性があります。
②当該製品にログインしたユーザーが悪意のある第三者によって細工されたページにアクセスした場合、当該製品に意図しない操作をさせられる可能性があります。(クロスサイトリクエストフォージェリ)

対処方法：
対策済みのファームウェアにアップデートを行い、問題を回避いたしました。
工場出荷時の設定では自動的に更新が行われます。
※設定を変更されているお客様は、下記を参照の上、対策をお願いいたします。

対象製品	対策済みファームウェアバージョン	対策	関連情報
WRC-2533GS2-B	Ver.1.69以降	ファームウェアのアップデート※1	① JVN#06672778
WRC-2533GS2-W			
WRC-2533GS2V-B			
WRC-X6000XS-G	Ver.1.12以降		①② JVN#06672778
WRC-X1500GS-B			
WRC-X1500GSA-B			

●不正アクセスでペイメントアプリ改ざん…ECサイトからカード情報約6.5万件等流出

https://www.itmedia.co.jp/news/articles/2408/01/news129.html
https://tokyotamagoofficial.com/information/2024/07/index.html

このニュースをザックリ言うと･･･

- 7月31日(日本時間)、菓子製造販売の東京玉子本舗より、同社公式オンラインショップが不正アクセスを受け、クレジットカード情報を含む個人情報が流出したと発表されました。

- 被害を受けたのは、2021年3月18日～2024年5月28日に同サイトでクレジットカード決済を行ったユーザー65,387件のクレジットカード情報(名義人名・番号・有効期限・セキュリティコード)と、2019年4月22日～2024年5月28日に同サイトを利用したユーザー73,961件の個人情報(氏名・住所・メールアドレス・電話番号・FAX番号・生年月日・性別・職業・購入履歴)とされています。

- 5月28日にサイト一部に改ざんの可能性があると連絡を受けサイトを閉鎖、6月20日までの第三者機関による調査の結果、システムの一部の脆弱性を突いてペイメントアプリケーションの改ざんが行われたことによる流出が発覚したとのことです。

AUS便りからの所感

- 近年のECサイトからのクレジットカード情報漏洩では、サーバー上にカード情報を保持しない仕様であったとしても、サイトの脆弱性を突いての決済アプリケーションやフォームの改ざんを行うことにより、セキュリティコードも含めたカード情報を外部に送信するような手口が主流となっています。

- ECサイト構築で利用される有名なフレームワークにおいてSQLインジェクション等の脆弱性が発見、修正されたにも拘らず、アップデートされていない状態のECサイトが攻撃を受けるケースも度々報告されており、攻撃者による侵入や改ざんの余地をなくすため、Webアプリケーション・フレームワークからサーバーに至るまで最新のバージョンに保ち脆弱性の修正・対策を確実に行うよう心掛けるとともに、攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置も検討してください。

ITmedia NEWS

「ごまたまご」公式ECサイトからカード情報6.5万件流出か　ペイメントアプリ改ざんで

2024年08月01日 13時58分 公開　[ITmedia]

東京土産として人気の「ごまたまご」「ニューヨークキャラメルサンド」などを販売する東京玉子本舗は7月31日、公式オンラインショップが不正アクセスを受け、顧客のクレジットカード情報約6.5万件を含む約14万件の個人情報が漏えいした可能性があると発表した。

システムの脆弱性をついた不正アクセスを第三者から受け、ペイメントアプリが改ざんされたことが原因という。

● 7月はWordPressのプラグインに48件の脆弱性報告…Sucuri社発表

https://news.mynavi.jp/techplus/article/20240805-2995801/
https://blog.sucuri.net/2024/07/wordpress-vulnerability-patch-roundup-july-2024.html
https://wpmake.jp/contents/knowledge/202407wp-news/

このニュースをザックリ言うと･･･

- 7月29日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、WordPressプラグインにおいて7月に報告された48件の脆弱性のまとめ記事が発表されました。

- 最も危険度が高い「Critical」にあたるのは「HUSKY」のSQLインジェクションおよび「Redux Framework」のクロスサイトスクリプティング(XSS)、次いで「High」にあたるのがSQLインジェクション1件、XSS3件、権限昇格1件となります。

- 危険度「Medium」「Low」についてはXSSが21件、不適切なアクセス制御の問題が11件、等となっています。

AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、4・5・6月分でそれぞれ43件・39件・40件の報告があります(ただし別の情報源ではここでまとめられていない脆弱性も報告されており、調査の際は複数の情報源をあたることが重要です)。

- WordPress本体においても6月にセキュリティアップデート6.5.5等がリリースされるなど、不定期に更新されることがあります。

- 本体・プラグインともインストールした状態のままで放置するようなことは決してせず最新に保つよう努めること、加えてセキュリティを強化するプラグインを必ずインストールすること、併せて(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入も検討に値します。

TECHR Powered by マイナビニュース

7月のWordPressプラグイン脆弱性まとめ、確認と対応を

掲載日 2024/08/05 08:28　著者：後藤大地

Sucuriはこのほど、「WordPress Vulnerability & Patch Roundup July 2024」において、2024年7月に明らかになったWordPressの脆弱性およびセキュリティパッチの情報について伝えた。Sucuriはウェブサイト所有者に対して新たな脅威を把握して対処してもらえるよう1か月間のWordPressエコシステムの重要なセキュリティアップデートと脆弱性パッチの一覧をまとめて公表している。