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。

●食品メーカーのECサイトからカード情報1,293件流出…不正アクセスによりWebアプリケーション改ざん

https://www.itmedia.co.jp/news/articles/2101/20/news116.html
https://www.kakiyasuhonten.co.jp/files/news/Press/pdf/20210119_info.pdf

このニュースをザックリ言うと･･･

- 1月19日(日本時間)、精肉・惣菜等を販売する柿安本店より、同社ECサイト「柿安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が流出したと発表されました。

- 流出した可能性があるのは、2020年4月29日～9月30日に同サイトで決済に使用されたクレジットカード情報(名義人名、番号、有効期限およびセキュリティコード(CVV))1,293件とされています。

- 2020年10月13日にクレジットカード会社からカード情報流出の懸念があるとの連絡を受けて決済を停止、同12月7日までに第三者調査機関による調査が行われ、流出および一部情報の不正利用の事実が確認されたとしています。

AUS便りからの所感等

- 流出の原因については「システムの一部の脆弱性をついたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われたため」としており、フォームから入力されたクレジットカード情報が攻撃者に送信されるよう仕向けられたものとみられます。

- ECサイトからのクレジットカード情報を奪取する手口については、以前は「サーバー上に保存・蓄積されていたカード情報を奪取する」ものも多くありましたが、クレジットカード業界団体によるガイドラインの策定により、基本的にサイト上ではセキュリティコードをはじめとするカード情報を保持しない(非保持化)方針が推し進められてからは、「カード情報の入力フォームを改ざんし、入力されたカード情報を奪取する」パターンが主流となっています。

- 上記2通りの手口のいずれにしても、大抵はWebサーバーやアプリケーションの脆弱性(SQLインジェクション・ディレクトリトラバーサル等)を突かれて行われるものであり、根本的対策として使用しているソフトウェアを最新のバージョンに保ち、また独自のWebアプリケーションの開発においても各種脆弱性が発生しないような開発体制をとること等が肝要であり、加えてそういった攻撃を受ける前に外部機関による診断を受ける、不正なリクエストを検知・遮断するソリューションを導入する等、各種対策をとって頂ければ幸いです。

ITmedia NEWS

不正アクセスでペイメントアプリ改ざん　「柿安オンラインショップ」カード情報集出、不正利用も

2021年01月20日 14時24分 公開　[ITmedia]

精肉や惣菜などを各地のデパートなどで販売する柿安本店は1月19日、ECサイト「柿安オンラインショップ」が不正アクセスを受けて顧客のクレジットカード情報が流出し、一部の顧客のカード情報が不正利用された可能性があると発表した。第三者によってシステムの脆弱性が突かれ、ペイメントアプリを改ざんされたためという。

カード情報が流出した可能性がある顧客は1293人で、2020年4月29日～9月30日に「柿安オンラインショップ」でカード決済した人。カード名義人名、カード番号、有効期限、セキュリティコードが漏えいしたおそれがあるという。

●複数のNEC製のWi-Fiルーターに脆弱性…「Aterm WF800HP」など、いずれも生産終了機種

https://internet.watch.impress.co.jp/docs/news/1302016.html
https://jpn.nec.com/security-info/secinfo/nv21-005.html

このニュースをザックリ言うと･･･

- 1月22日(日本時間)、IPAとJPCERT/CCより、NEC製のWi-Fiルーター「Aterm」シリーズの一部製品に脆弱性が存在するとして注意喚起が出されています。

- 脆弱性が存在する機種(ファームウェアのバージョン)は、いずれも生産終了機種の「Aterm WF800HP(ファームウェア バージョン1.0.19以前)」「WG2600HP(同1.0.2以前)」「WG2600HP2(同1.0.2以前)」で、いわゆるクロスサイトスクリプティング(XSS)やクロスサイトリクエストフォージェリ(CSRF)により、ルーターにログインしている管理者等に不正な処理を実行させるよう誘導することが可能とのことです。

- NECではWG2600HP・WG2600HP2について最新バージョンのファームウェアへアップデートすることを呼び掛けており、また今回の脆弱性についての修正が提供されていないWF800HPについては、脆弱性の回避策として「ウェブサイトにアクセスする場合には、信頼できる情報源から URL を取得してアクセスしたあと、お気に入りに登録し、2回目以降のアクセスは、登録済みのお気に入りから行う」ことを推奨しています。

AUS便りからの所感

- WG2600HP・WG2600HP2等のファームウェアにおける脆弱性の修正は2019年の時点で行われており、自動更新機能もデフォルトで有効ですが、最新バージョンであるか確認を行い、意図的に無効にしているのであれば確実にアップデートを行うようにしてください。

- WF800HPについては前述した2019年の時点で修正を行ったことは明言されておらず(一方でファームウェアの最新バージョンは1.0.22となっている等、情報が錯綜しているきらいもあります)、また2013年6月の発売から7年半近く経過していることから、可能であれば新しい機種へのリプレースを計画すべきでしょう(既に生産終了している他の2機種についても、数年後の実施を前提としたリプレースの計画を立てることは検討に値すると思われます)。

- その他のベンダー製品も含め、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・終了したと見られる機種を適宜新しいものと交換する体制を整えることが重要です。

Impress Watch

複数のNEC製のWi-Fiルーターに脆弱性、生産終了した「Aterm WF800HP」など
「Aterm WG2600HP」「Aterm WG2600HP2」も対象

磯谷 智仁　2021年1月25日 12:04

NECプラットフォームズ株式会社が提供する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。

脆弱性の影響を受けるのは、生産を終了した以下3製品になる。

- 「Aterm WF800HP」ファームウェア バージョン1.0.19以前
- 「Aterm WG2600HP」ファームウェア バージョン1.0.2以前
- 「Aterm WG2600HP2」ファームウェア バージョン1.0.2以前

●「あなたのメールアドレスはまもなく期限切れになります」…さくらインターネットを騙るフィッシングに注意喚起

https://www.itmedia.co.jp/news/articles/2101/22/news122.html
https://help.sakura.ad.jp/notification/360000338410228/

このニュースをザックリ言うと･･･

- 1月22日(日本時間)、レンタルサーバー・クラウドサービスなどを提供するさくらインターネット社より、同社を騙るフィッシングが出回っているとして注意喚起が出されています。

- フィッシングの一例として、差出人が「さくらインターネット <SAKURA@help.sakura.japan>」、件名が「重要？あなたのメールアドレスはまもなく期限切れになります」で、本文が「親愛な***@*****(相手のメールアドレス)」で始まり、同社サービスの偽のログイン画面へ誘導するものが挙げられています。

- 同社では、不審なメールを受け取っても本文中のリンクへのアクセスを絶対に行わない、アクセス先でID・パスワードなどを入力しない等を呼び掛けています。

AUS便りからの所感

- フィッシングサイトは本物のログイン画面の画像を張り付けた上に偽のフォームを設置しているもので、試しに適当な情報を入力すると本物のさくらインターネットのサイトに遷移するようになっていましたが、ユーザーによっては騙されてログイン情報を入力してしまった後でも気づきにくいケースもあると考えられます。

- 注意喚起では、誤ってアカウント情報を入力した場合の対処についても解説、場合によっては会員IDの変更も行うよう呼び掛けるとともに、サービスを安全に利用するために2段階認証を設定することも推奨しています。

- さくらインターネット社が挙げている以外のユーザー側の自衛策としては、利用しているサービスのサイトには事前に登録したブックマークからアクセスすることが効果的で、加えてアンチウイルス・ブラウザー・UTM等のアンチフィッシング機能を有効にすることも有用でしょう。

ITmedia NEWS

さくらインターネットかたる詐欺メールに注意　個人情報の窃取やサーバ不正利用の恐れ

2021年01月22日 16時01分 公開　[ITmedia]

さくらインターネットは1月22日、同社をかたるフィッシングメールが出回っているとして注意を呼び掛けた。遷移先の偽サイトからIDやパスワードが窃取されると、不正ログインによって個人情報の取得やWebサイトの改ざんなどの恐れがあるとしている。

件名

重要 - あなたのメールアドレスはまもなく期限切れになります

本文の特徴

親愛な ***@*****　※1