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。

●XSS攻撃で決済フォーム改ざんか…約5,200件の個人情報・クレカ情報流出

https://scan.netsecurity.ne.jp/article/2024/02/07/50564.html
https://fineaid.co.jp/shop/information/2024-01-31

このニュースをザックリ言うと･･･

- 1月31日(日本時間)、株式会社ファインエイドより、同社が運営する「健康いきいきライフスタイル」のWebサイトが外部から攻撃を受け、一部利用者のクレジットカード情報を含む個人情報が流出した可能性があると発表されました。

- 被害を受けたとされるのは、2021年1月5日～2023年11月15日に同サイトを利用した利用者5,193人分の個人情報(氏名・住所・メールアドレス・電話番号・FAX番号・注文履歴・生年月日・性別)およびクレジットカード情報(名義人名・カード番号・有効期限・セキュリティコード)とされています。

- 2023年12月11日にカード会社からの連絡を受けて同12日にカード決済を停止、第三者機関による調査の結果、同26日に流出の可能性が確認されたとしています。

AUS便りからの所感等

- 流出の原因としては、サイトのシステムに存在していたクロスサイトスクリプティング(XSS)の脆弱性を悪用され、決済のためのアプリケーションが改ざんされたためとしています。

- XSSによる攻撃はサイトへの訪問者に対して行うパターンだけでなく、管理画面に出力される登録情報・注文内容およびログ等に不正な文字列を仕込むことにより、閲覧した管理者の権限で不正なスクリプトを実行させるパターンもあり、2021年4月には国内ECサイトで実際にこのパターンの攻撃による管理者アカウント情報・カード情報等の奪取を狙った攻撃が確認され、JPCERT/CC等から注意喚起が出されています(https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html)。

- 今回のケースで行われたXSS攻撃の詳細な情報は出ていませんが、不特定多数がアクセスする表側はもちろん、管理画面においても各種情報の出力を安全に行うようWebアプリケーション上での根本的な対策は不可欠です。


ScanNetSecurity

インシデント・事故／インシデント・情報漏えい

2024.2.7 Wed 8:05

「健康いきいきライフスタイル」に不正アクセス、5,193 名のカード情報が漏えい

株式会社ファインエイドは1月31日、同社が運営する「健康いきいきライフスタイル」への不正アクセスによる個人情報漏えいについて発表した。

シェア　ポスト　送る

株式会社ファインエイドは1月31日、同社が運営する「健康いきいきライフスタイル」への不正アクセスによる個人情報漏えいについて発表した。

公式サイト

全４枚

拡大写真

これは2023年12月11日に、一部のクレジットカード会社から「健康いきいきライフスタイル」を利用した顧客の個人情報の漏えい懸念について連絡があり、翌12月12日に当該サイトでのカード決済を停止し、第三者調査機関による調査を開始したところ、当該サイトのシステムの一部の脆弱性を悪用したクロスサイトスクリプティングの手法による第三者の不正アクセスで、サーバ内にクレジットカード決済実行時に処理される個人情報を取得するためのアプリケーションの改ざんが行われたことが原因で、顧客の個人情報が漏えいした可能性を2023年12月26日に完了した調査結果で確認したというもの。

●厚労省内部メーリングリストでアドレスの誤登録、個人情報・公開前内部資料等流出

https://www3.nhk.or.jp/news/html/20240202/k10014344861000.html
https://www.mhlw.go.jp/stf/newpage_37720.html

このニュースをザックリ言うと･･･

- 2月2日(日本時間)、厚生労働省より、省内のメーリングリスト(ML)に誤って外部の第三者のメールアドレスが登録され、内部情報がメールで送信されていたと発表されました。

- 同省の発表によれば、2023年9月15日～2024年1月23日にかけて、行政機関職員650名分のメールアドレスおよび民間人25名分の電話番号がMLから第三者に送信される状態にあったとしており、加えて一部報道によれば、岸田総理大臣の国会答弁案や公表前の内部資料も同様に外部へ送信されていた模様です。

- 同省職員が、夜間・休日の緊急連絡先として私用のメールアドレスを登録しようとした際に誤登録が発生したのが原因としており、再発防止策として「テレワーク環境の改善を踏まえ、本省における私用メールアドレスの業務上の使用については、禁止する」としています。

AUS便りからの所感

- 職員は夜間・休日においてもリモートアクセスで公務用の内部メールアドレスを使用した対応を行っており、(本来MLの登録が想定されていた)私用のメールアドレスにメールが届いているかを確認していなかったとし、発表ではこれが誤登録の確認が遅れた要因としています。

- 一方で、リモートアクセスと内部メールアドレスによるメール送受信の実施を徹底し、同時にMLからのメール配信を組織内ドメイン名のメールアドレスに限定することは、私用メールアドレス等外部へのメール送信による情報の流出の可能性を抑止することが期待できるという意味では、一定の効果が見込まれるとみられます。

NHK

厚労省のMLに誤アドレス登録しメール誤送信 首相答弁案も流出

2024年2月2日 16時27分　厚生労働省

厚生労働省の職員が、省内のメーリングリストに誤ったアドレスを登録し、去年9月以降、岸田総理大臣の国会答弁案や、民間と行政の職員675人分の個人情報などが誤送信されていたことがわかりました。
今のところ情報が悪用されるなどの被害は確認されていないということですが厚生労働省は、再発防止に努めるとしています。

● auの古いWi-Fiルーターに脆弱性…サポート終了のためアップデートなし

https://scan.netsecurity.ne.jp/article/2024/02/08/50567.html
https://jvn.jp/vu/JVNVU93740658/index.html
https://www.au.com/support/service/mobile/guide/wlan/home_spot_cube_2/

このニュースをザックリ言うと･･･

- 2月2日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、KDDIがauユーザーに提供していたWi-Fiルーター「HOME SPOT CUBE2」に脆弱性が確認されたとして注意喚起が出されています。

- 脆弱性(CVE-2024-21780・CVE-2024-23978)は、外部から不正なリクエスト等を送信することにより、サービス拒否(DoS)状態に陥ったり、任意のコードを実行され、機器を乗っ取られたりする恐れがあるとされています。

- 当該機器は2022年9月にKDDIによるサポートが終了しており、アップデートの提供予定はないとのことです。

AUS便りからの所感

- JVNでは回避策として「本製品は、信頼できるネットワークにのみ接続する」ことを挙げています。

- ルーターやIoT機器の脆弱性は他のメーカーにおいても度々報告されており、攻撃者はあらゆる機器の脆弱性情報をもとに日々アップデートを行っていない機器を検索し、攻撃あるいはその準備を行っていると考えられるため、外部ネットワークから管理画面等にアクセス可能な状態にある物を含めあらゆるIoT機器・ネットワーク機器についてその存在を把握して管理すること、ファームウェアのアップデートが提供されているものは必ず最新バージョンに保つこと、一方でアップデートの提供が終了している機器は確実にリプレースする体制をとることが重要です。

ScanNetSecurity

脆弱性と脅威／セキュリティホール・脆弱性

2024.2.8 Thu 8:00

HOME SPOT CUBE2 に複数のバッファオーバーフローの脆弱性

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2月2日、HOME SPOT CUBE2における複数のバッファオーバーフローの脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。

シェア　ポスト　送る

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2月2日、HOME SPOT CUBE2における複数のバッファオーバーフローの脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。株式会社ゼロゼロワンの早川宙也氏が報告を行っている。影響を受けるシステムは以下の通り。

HOME SPOT CUBE2 V102 およびそれ以前

KDDI株式会社が提供するHOME SPOT CUBE2には、下記の影響を受ける可能性がある複数のバッファオーバーフローの脆弱性が存在する。