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。

●カステラ販売サイトから709人分のクレカ情報流出

https://this.kiji.is/754533321931587584
https://shop.ijindo.co.jp/info.pdf

このニュースをザックリ言うと･･･

- 4月12日(日本時間)、カステラ製造販売業の異人堂より、同社が運営するショッピングサイト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。

- 被害を受けたのは、2019年11月29日～2020年11月20日の間に同サイトでクレジットカード決済を行った購入者709名・738件分の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))とされています。

- 2020年11月20日に、クレジットカード会社からカード情報流出の懸念について連絡を受け決済を停止しており今年2月26日までに第三者機関による調査が行われた結果、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も送信されるよう仕向けられたものとみられます。

- ECサイト上でのクレジットカードの扱いについて「サイト上でカード情報を保持するにはPCI DSSに準拠する」さもなくば「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)」とするガイドラインが2016年にカード業界団体において策定されたことを受け、多くのECサイトは決済代行業者と契約する等して自前での非保持化を選択したとみられ、現在におけるECサイトからのクレジットカード情報を奪取する手口は、「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」ものから「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」ものへと主流が移行しています。

- ただし、これらの手口はいずれも、Webサーバー・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点で共通しており、根本的対策として、使用している各ソフトウェアを最新のバージョンに保つこと、また独自のWebアプリケーションの開発において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。

長崎新聞

異人堂　情報漏えいか　顧客709人分のクレジットカード情報　長崎

2021/4/13 11:27 (JST)　　©株式会社長崎新聞社

カステラ製造販売業の異人堂（長崎市）は12日、運営するショッピングサイトが不正アクセスを受けたと同社ホームページで発表した。顧客709人分、計738件のクレジットカード情報が漏えいし、一部は不正利用された可能性があるとしている。

同社によると、昨年11月20日、カード会社から情報漏えいの疑いがあると連絡があり、同サイトでの決済を停止。調査の結果、2019年11月29日から20年11月20日までの間、同サイト利用者のカード情報（名義人名、カード番号、有効期限、セキュリティーコード）が漏えいした可能性があることが判明した。

●カプコン不正アクセスの調査結果公表…古いVPN装置への侵入が原因

https://www.asahi.com/articles/ASP4F6FQSP4FPLFA00C.html
https://www.capcom.co.jp/ir/news/html/210413.html

このニュースをザックリ言うと･･･

- 4月13日(日本時間)、カプコン社より、昨年11月に発表された同社への不正アクセス事案(AUS便り 2020/11/16号)についての最新の調査結果が発表されました。

- 侵入の原因として、同社の北米現地法人が保有していたVPN装置に古いものがあり、その脆弱性を悪用されたためとされています。

- なお、この不正アクセスによるユーザーのクレジットカード情報の流出はなく、ユーザーのゲームプレイやダウンロードにも影響はないとしており、また攻撃を行った犯罪グループからの身代金要求にも応じていないとのことです。

AUS便りからの所感

- 当該現地法人含めグループ各社においては既に新たなVPN装置を導入済みでしたが、コロナ禍に起因するネットワーク負荷増大に伴い、通信障害等が発生した際の緊急避難用として古いVPN装置1台が残存していたとのことで、当該装置は現在廃棄済みとのことです。

- 2020年3月に米政府機関がテレワーク(リモートワーク)実施におけるセキュリティリスクに対し注意喚起を行った(AUS便り 2020/3/23号)際にはVPN装置への攻撃が重要な要素として挙げられており、またVPNの需要が急増する直前の2019年にも、複数メーカーのVPN装置に脆弱性が報告され、攻撃の恐れに対する注意喚起がJPCERT/CC等から出ていました(同 2019/9/24号参照)。

- 今回はあえて古い機器を残していたという事情がありましたが、システム管理者が設置を把握していない古い機器が侵入経路となるケースもまた多いものと考えられるため、そういった管理下にない機器が内部LAN上の他のPC等あるいは外部の指令サーバー等と通信を行わないような各種対策を実施するよう検討すべきです。

朝日新聞 DIGITAL

「旧型VPN機器に攻撃」 カプコン、情報漏洩で報告書

会員記事

森田岳穂、橋本拓樹　2021年4月13日 19時28分

シェア　ツイート list　ブックマーク 4　メール　印刷

カプコン本社=大阪市中央区

ゲーム大手の カプコン（大阪市）は13日、サイバー犯罪 グループが絡んだ 情報漏洩（ろうえい）問題についての調査結果を公表した。旧型の仮想プライベートネットワーク（VPN）機器が攻撃を受け、社内ネットワークに侵入されたとみられるなどと説明。対策が脆弱（ぜいじゃく）な部分を標的にされたことを明らかにした。

発表によると、サイバー攻撃 を受けたのは昨年10月前半。同社の米国の現地法人が使う旧型のVPN機器が対象となった。社内ネットワークに侵入され、取引先や社員の氏名や住所、電話番号など最大約38万人分の個人情報が漏洩した可能性があるという。攻撃を確認した同11月2日以前の段階では、システム障害は確認されなかったという。

●グルメ情報サイトのスマホアプリに脆弱性、フィッシング悪用の可能性も…アップデートを

https://www.itmedia.co.jp/news/articles/2104/15/news128.html
https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-000031.html

このニュースをザックリ言うと･･･

- 4月14日(日本時間)、IPAおよびJPCERT/CCより、グルメ情報サイト「ぐるなび」のスマートフォンアプリに脆弱性が存在するとして注意喚起が出されています。

- 脆弱性はAndroid版アプリ(バージョン10.0.10以前)とiOS版アプリ(バージョン11.1.2以前)双方に存在するとされ、攻撃者により、このアプリから任意のサイトにアクセスするよう仕向けられ、フィッシング詐欺等の被害を受ける可能性があるとされています。

- 各アプリについて脆弱性を修正したバージョンがリリースされており、アップデートを強く推奨されています。

AUS便りからの所感

- 脆弱性はカスタムURLスキーム(URLの先頭がhttps:// 等ではない、アプリが独自に処理するように設定されるもの)の処理におけるもので、アプリに関連付けられたカスタムURLスキームを含む細工されたURLへのアクセスにより、URLがアプリに渡され、アプリ内のブラウザーが任意のサイトにリダイレクトする可能性があり、攻撃者はその場面でぐるなびのページを騙るフィッシングサイトに誘導する等を行うことが可能とみられています。

- Android・iOSとも自動的あるいは手動でアプリのアップデートを行う機能が備わっていますので、もし手動でアップデートする設定であったならば、当該アプリが既に安全なバージョンであるかの確認、またはアップデートの通知が来ていることの確認とその適用を必ず行うようにしてください。

ITmedia NEWS

「ぐるなび」アプリに脆弱性、フィッシング詐欺被害の恐れ　「最新版へ更新を」IPAが呼び掛け

2021年04月15日 19時27分 公開　[ITmedia]

印刷　見る　Share　B! 8

スマートフォンアプリ「ぐるなび」（iOS／Android、無料）にアクセス制限の不備があり、フィッシング詐欺などの被害にあう恐れがあるとして、IPA（情報処理推進機構）とJPCERT/CC（JPCERTコーディネーションセンター）は4月14日、アプリを最新版にアップデートするよう注意を促した。