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。

●EC-CUBEバージョン4系にクロスサイトスクリプティングの脆弱性…アップデートを

https://netshop.impress.co.jp/node/8692
https://www.ec-cube.net/news/detail.php?news_id=383
https://www.ipa.go.jp/security/ciadr/vul/20210510-jvn.html

このニュースをザックリ言うと･･･

- 5月7日(日本時間)、イーシーキューブ社(以下・同社)より、同社開発のECサイト構築用ソフトウェア「EC-CUBE」にクロスサイトスクリプティング(XSS)の脆弱性が発見されたとして注意喚起が出されています(同10日にはIPA・JPCERT/CCからも同様に注意喚起が出されています)。

- 脆弱性はEC-CUBEのバージョン4.0.0以降に存在(バージョン3系・2系には存在しないとのことです)し、不正な入力内容を含む受注等が行われた際、ECサイトの管理画面でそれを表示することにより、不正なスクリプトの実行等が行われる恐れがあるとされています。

- 同社では、既に脆弱性を悪用した攻撃も確認されているとし、4系のユーザーに対し最新バージョン4.0.5-p1へのアップデート(あるいは脆弱性の修正パッチの適用)を強く推奨しています(クラウド版については対策済みとのことです)。

AUS便りからの所感等

- XSSの脆弱性は、不正なパラメータを含むURLへターゲットを誘導する等で発動する「Reflected XSS(反射型XSS)」と、今回のような「Stored XSS(格納型・持続型XSS)」に分類され、後者のケースではWebサイトを普通に利用する不特定多数のユーザーに対しても影響を及ぼすことも珍しくありません。

- EC-CUBEについては2019年12月にも古いバージョンの脆弱性を悪用した攻撃について注意喚起が出されていました(AUS便り 2020/1/14号参照)が、今回は最も新しいバージョンである4系でのみ存在する脆弱性となることに注意が必要です。

- 今回の脆弱性を悪用した攻撃により、クレジットカード情報が流出したケースもあるとのことで、EC-CUBEを導入しているサイトの管理者においては、速やかに同社の注意喚起を参照するとともに、掲載されている情報をもとに、EC-CUBEのバージョンと対策の要・不要およびサイトにおいて攻撃された痕跡がないかを確認し、適宜対策をとって頂ければ幸いです。

impress BUSINESSMEDIA

「EC-CUBE 4.0系」で緊急度「高」の脆弱性、該当するECサイトは緊急対応を

開発元のイーシーキューブは複数サイトでの攻撃を確認。脆弱性を悪用したクレジットカード情報の流出を確認しているという

5月11日 13:00 シェア 28 ツイート 13 B! はてブ noteで書く

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は5月10日、オープンソースECサイト構築パッケージ「EC-CUBE 4.0系」で、緊急度「高」の脆弱（ぜいじゃく）性が発覚したことによる注意喚起を行った。

「EC-CUBE」のWebサイトより

開発元のイーシーキューブは5月7日にクロスサイトスクリプティング（Webサイトのアプリケーションの脆弱性を悪用した攻撃）の脆弱性（CVE-2021-20717）に関する情報を公開。「緊急度が非常に高い脆弱性」と注意喚起をしている。

脆弱性が悪用された場合、ECサイトの管理者のブラウザ上で任意のスクリプトが実行され、ECサイトへの不正アクセスや個人情報の搾取などが行われる可能性がある。

イーシーキューブは複数サイトでの攻撃を確認。脆弱性を悪用したクレジットカード情報の流出を確認しているという。

該当するのは「EC-CUBE」のバージョンが4.0.0～4.0.5で、利用している企業向けに、緊急対応のためのHotfixパッチを公開。早期のパッチ適用といった対応をアナウンスしている。

●Wi-Fiセキュリティプロトコルに複数の脆弱性、ほぼ全ての機器に影響か…HTTPS・VPN等の使用を

https://internet.watch.impress.co.jp/docs/news/1324389.html
https://jvn.jp/vu/JVNVU93485736/
https://www.fragattacks.com/

このニュースをザックリ言うと・・・

- 5月12日(日本時間)、ベルギーのセキュリティ研究者Mathy Vanhoef氏より、Wi-Fiセキュリティプロトコルに複数の脆弱性が存在すると発表され、JPCERT/CC等からも相次いで注意喚起が出されています。

- 「FragAttacks」と名付けられた計12件の脆弱性は、1997年発表の「WEP」から現行最新の「WPA3」までのWi-Fiセキュリティプロトコルに影響し、ほぼ全てのWi-Fi機器(スマートフォン・タブレット・ノートパソコン・ルーター他)が何らかの影響を受けるとみられています。

- 無線LANの通信範囲内にいる攻撃者による、通信の改ざんや読み取りが可能になるとされ、Vanhoef氏による解説用のWebサイトにおいても、機密情報の奪取や、スマート家電の不正操作およびそれを経由してのWindows 7搭載PCへの侵入といったデモンストレーション動画が示されています。

AUS便りからの所感

- 今回FragAttacksについて発表したVanhoef氏は、2017年にもWAP・WPA2に関する複数の脆弱性「KRACKs」(AUS便り 2017/10/23号参照)を、2019年には前年に発表されたばかりのWPA3に関する複数の脆弱性「Dragonblood」を発表しています。

- 12件のうち3件はWi-Fiの規格「IEEE 802.11」の設計上の欠陥、残り9件は実装上の不備により起こり得るものとされ、前者の悪用にはターゲットとなるユーザー側での特別な操作あるいは一般的でない設定が前提となり、現時点で実際に影響を受ける可能性は低いとしている一方、後者についてユーザーが知らない間に悪用される可能性が懸念されている模様です。

- Windowsでは既にセキュリティアップデートにおいて一部が対策されており、AndroidやiOS等他の製品においても脆弱性の有無の発表およびセキュリティアップデートのリリースが望まれますが、KRACKsの時と同様、HTTPSやVPN等別途の暗号化通信を、社内外での無線LAN通信において確実に行うことが重要でしょう。

Impress Watch

全Wi-Fi機器に影響する脆弱性「FragAttacks」発見される。各企業・団体が対応を発表

山田 貞幸　2021年5月14日 14:46

ニューヨーク大学アブダビ校のMathy Vanhoef氏は12日（日本時間）、「すべてのWi-Fi機器が影響を受ける」Wi-Fiの設計と実装に関する複数の脆弱性が見つかったと発表した。「FragAttaks（fragmentation and aggregation attacks）」と名付けられ、内容の詳細はfragattacks.comで公開されている。

発見されたのは、WPA3を含む、Wi-Fiの全ての最新のセキュリティプロトコルに影響を及ぼすもの。ほとんどのデバイスに影響するWi-Fi標準「IEEE 802.11」の設計上の欠陥に起因する3件（CVE-2020-24586、CVE-2020-24587、CVE-2020-24588）や、Wi-Fi製品のプログラミングのミスにより引き起こされるものなど、全12件の脆弱性。

発見されたデバイスの脆弱性を直接悪用することは、特殊な設定などが必要となるため困難とされる。しかし、Wi-Fi製品のプログラミングのミスによる脆弱性によりユーザーが知らない間に悪用される可能性があり、このことが最大の懸念事項であるとしている。

●大学病院の患者586人分の情報流出か…クラウドへのデータ同期とフィッシングによるパスワード奪取が原因

https://scan.netsecurity.ne.jp/article/2021/05/07/45622.html
https://mainichi.jp/articles/20210501/ddl/k12/040/026000c
https://www.ho.chiba-u.ac.jp/hosp/info/20210430info.html

このニュースをザックリ言うと・・・

- 4月30日(日本時間)、千葉大学医学部附属病院より、職員がフィッシング攻撃を受けたことがきっかけで、同病院患者の個人情報が外部から閲覧可能な状態となっていたことが発表されました。

- 被害を受けたのは同病院患者586人分の個人情報(ID・氏名・性別・生年月日・入退院日・診断名・入院目的他)とされています。

- 当該職員が大学の規定に反してデータを個人用PCに保存、さらに外部クラウドサービスにもデータが同期されていたところ、同25日に当該職員に対し宅配業者を騙るフィッシングメールがあり、クラウドサービスのID・パスワードを詐取されたとしています。

AUS便りからの所感

- 同病院では「個人所有のパソコンに患者様の個人情報を保存してはいけないこと」「やむを得ず保存する際には個人情報を匿名化すること」等の啓発・教育を行っていたものの、今回のケースではそれが徹底されていなかったとのことです。

- 「匿名化されていないデータの持ち出し」「意図しないとみられるクラウドサービスへのデータ同期」「フィッシング攻撃」と、複数の要素によって成立した事案であり、各企業・組織においてこの事例をもってのさらなる啓発・教育を行うにあたっては、どれか1つではなく全てについて注意を払うよう喚起する一方で、ユーザー側の注意に依存することなく、システム側でも事故に至る要因の発生を可能な限り抑えられるよう対策(今回であれば、匿名化されたデータを出力する機能を提供する、等)を検討するのが良いでしょう。

ScanNetSecurity

インシデント・事故 ／ インシデント・情報漏えい　2021年5月7日（金）08時05分

千葉大学医学部附属病院職員が宅配便騙るスミッシング被害、個人PCに保存した患者個人情報が閲覧可能に

国立大学法人千葉大学医学部附属病院は4月30日、同院職員が宅配業者を装ったフィッシングメールによりクラウドサービス用ID・パスワードを窃取され、患者の個人情報が閲覧できる状態になったことが判明したと発表した。

国立大学法人千葉大学医学部附属病院は4月30日、同院職員が宅配業者を装ったフィッシングメールによりクラウドサービス用ID・パスワードを窃取され、患者の個人情報が閲覧できる状態になったことが判明したと発表した。

これは同院職員が大学の規定に反し、患者の個人情報を個人用パソコンに保存し、大学で許可されていないクラウドサービスを利用していたところ、4月25日に宅配業者を装ったフィッシングメールにより当該クラウドサービスのID・

トップページ

リリース（患者情報の管理に関するご報告とお詫び）

シェア　ツイート

記事一覧：情報漏えい事故　原因別
記事一覧：不正アクセス