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。

●数億台以上のネットワーク機器に影響か…脆弱性「Ripple20」が発見される

https://gigazine.net/news/20200617-ripple20-vulnerabilities/
https://www.jsof-tech.com/ripple20/

このニュースをザックリ言うと・・・

- 6月16日(現地時間)、セキュリティ企業のJSOF社より、複数メーカー製のIoTデバイス・ネットワーク機器等に影響する19件の脆弱性が存在するとして注意喚起が出されています。

- 「Ripple20」と名付けられた一連の脆弱性は、米国のTreck社が開発したTCP/IP通信用ライブラリに存在するもので、当該ライブラリを使用する機器を外部から乗っ取ったり、機能停止させたりすることも可能になるとされています。

- 通信・小売・商社・医療・輸送・工業・エネルギー等広範囲の業界で使用される、全世界で数億台以上の機器が当該ライブラリを使用し、脆弱性の影響を受けるとされている一方、Treck社によれば既にメーカー向けに修正パッチをリリースしているとのことです。

AUS便りからの所感等

- JSOF社のデモンストレーションでは、ネットワークに接続するプリンターやUPS、あるいは輸液ポンプ等が脆弱性の悪用により停止する恐れがあることが示されています。

- 世界最大のネットワーク機器メーカーであるシスコシステムズ社が、詳細は調査中ながらも同社製品が脆弱性の影響を受けるとしており、また国内でも、以前Treck社と提携していた図研エルミック社より、同社が提供するライブラリに同種の脆弱性が存在すると発表されています(https://www.elwsc.co.jp/news/4136/)。

- 影響を受ける機器については今後ベンダーより順次情報が発表されるとみられますので、情報を随時確認の上、ファームウェアの更新が必要なケースでは必ず更新を行いましょう。

- 外部から直接攻撃を受けるケース以外に、内部からのDNSサーバー等への問合せに対し攻撃者から不正な回答を行うことによる攻撃が行われるケース等も考えられるため、そういったケースにも十分対応できるようUTMの設置さらにはクライアントPCやネットワーク機器との間で適切な隔離等を行うことを推奨致します。

GIGAZINE

2020年06月17日 11時32分　セキュリティ

数億台以上の電化製品にひそむ脆弱性「Ripple20」が発見される

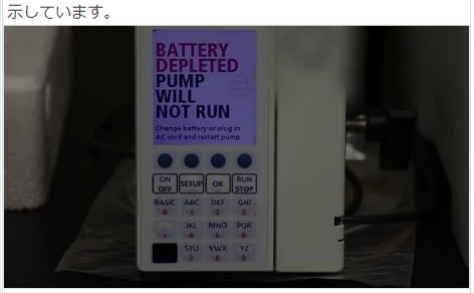
Ripple20

19 Zero-Day Vulnerabilities Amplified by the Supply Chain

セキュリティ企業JSOFが、IntelやHPの製品を含む多くのスマートデバイスやルーター、プリンターなどが影響を受ける脆弱性「**Ripple20**」を発見したと発表しました。Ripple20は、1997年にリリースされて以来多くのメーカーが採用してきたインターネット通信プロトコルのライブラリが原因となっていることから、この脆弱性の影響を受ける製品は全世界に数億台以上あると見られています。

UPSに電力が残っているにもかかわらず、照明器具の電源が落ちて暗くなってしまいました。

輸液ポンプも、バッテリー残量がないことを警告する画面を表示しています。



●「カメラのキタムラ」通販サイトに「リスト型攻撃」…個人情報40万件が閲覧された可能性

https://www.itmedia.co.jp/news/articles/2006/15/news138.html
https://www.kitamura.jp/topics/2020/20200615_01.html

このニュースをザックリ言うと・・・

- 6月15日(日本時間)、写真用品やスマートフォンの販売・修理チェーン店「カメラのキタムラ」より、同社の通販サイト「カメラのキタムラネットショップ」において約40万件の不正ログイン被害が発生したと発表されました。

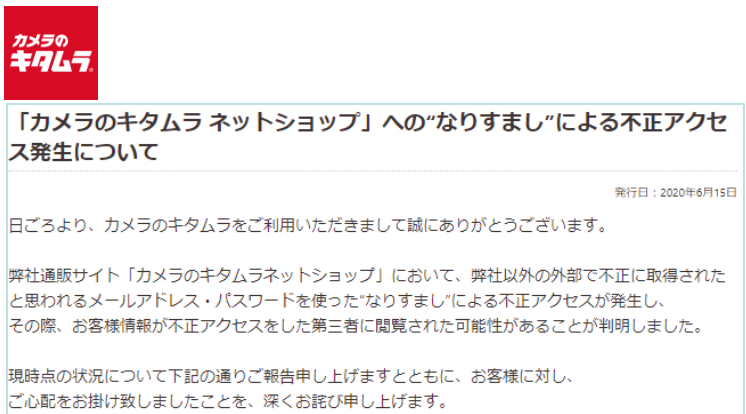
- 発表によれば、不正ログインは、海外のIPアドレスから、他のWebサイトで流出したアカウント情報を悪用した、いわゆる「リスト型攻撃」によって行われているとされ、個人情報(氏名・住所・生年月日・電話番号・メールアドレス・注文履歴等)が閲覧された可能性もあるとされています(クレジットカード情報は含まず)。

- 少なくとも4月4日以降から不正ログインが発生していることが5月28日に判明、対象ユーザーについてログインパスワードの初期化を行ったとしています。

AUS便りからの所感

- 前述の通り「リスト型攻撃」によるもので、アカウント情報が同社サーバーから流出したものではないとされる一方、二段階認証による不正ログイン対策あるいはreCAPTCHAによる自動的なログインへの対策を行っておらず、同社では今後可能なものから早急に実装するとしています。

- ユーザー側においては、複数のサービス間で全く同じパスワードを使い回さず、また推測されやすい簡単なパスワードを設定することもないよう注意し、今後も不正ログイン発生時に備え、各サービスに登録しているアカウント全てについて漏れなく管理を行うことが肝要です。



カメラのキタムラ

「カメラのキタムラ ネットショップ」への"なりすまし"による不正アクセス発生について

発行日：2020年6月15日

日ごろより、カメラのキタムラをご利用いただきまして誠にありがとうございます。

弊社通販サイト「カメラのキタムラネットショップ」において、弊社以外の外部で不正に取得されたと思われるメールアドレス・パスワードを使った"なりすまし"による不正アクセスが発生し、その際、お客様情報が不正アクセスをした第三者に閲覧された可能性があることが判明しました。

現時点の状況について下記の通りご報告申し上げますとともに、お客様に対し、ご心配をお掛け致しましたことを、深くお詫び申し上げます。

● Adobe、Flash Playerの12/31終了を改めて告知

https://gigazine.net/news/20200616-flash-player-end-of-life/
https://www.adobe.com/jp/products/flashplayer/end-of-life.html

このニュースをザックリ言うと・・・

- 6月16日(日本時間)、Adobe社より、同社による「Flash」および「Flash Player」の開発・提供が12月31日で終了することが改めて告知されています。

- Flash Playerに危険度の高い脆弱性が多く報告されることや、HTML5等の新しい代替技術の普及を鑑み、同社からは2017年7月の時点で提供の終了が発表され、既存のFlashコンテンツを代替技術を用いたものに切り替えるよう呼び掛けられていました(AUS便り 2017/7/31号参照)。

- 上記の流れについてはMicrosoft・Google・Mozilla・Apple等も協力しており、各種WebブラウザーにおいてFlash Playerのサポート終了について警告を出したり、Flashコンテンツをデフォルトでブロックしたりする挙動がとられています。

AUS便りからの所感

- 6月9日にはFlash Playerのセキュリティアップデートがリリースされている(https://news.mynavi.jp/article/20200611-1052351/)等、Adobe社では提供終了までの間、引き続きサポートを行うとしており、各PCにインストールされているFlash Playerを確実に最新のバージョンに保つことが最も重要です(通常は自動更新で最新にアップデートします)。

- 企業等のWebサイト側においても、古いFlashコンテンツを未だに使っている場合、2021年以降は基本的にブラウザーから利用できなくなりますので、今からでもコンテンツを新しいものに置き換えるよう計画する必要があります。

- Flashコンテンツのみが危険というわけでは決してなく、悪意のあるJavaScript等が改ざんされたWebサイトや不正な広告配信で実行される恐れがあることにも十分に注意し、アンチウイルス・UTM等による防御も忘れず行うべきです。

Adobe Flash Playerサポート終了情報ページ

1. Flash Playerのサポートが終了するのはいつですか？

2017年7月に発表しましたとおり、2020年12月31日をもってアドビによるFlash Playerの配布と更新を終了します。この発表はアドビのテクニカルパートナー数社（Apple、Facebook、Google、Microsoft、Mozillaなど）と協調しておこない、パートナー各社は、提供するOS環境またはブラウザーを使用しているデベロッパー、法人、消費者にとってFlash Playerのサポート終了がどのような影響があるかについて、技術的な詳細を含む補足的発表をおこないました。

2. アドビがなぜFlash Playerのサポートを終了し、2020年末までとしたのですか？

HTML5、WebGL、WebAssemblyなどのオープンスタンダードが年月を経て安定的に成熟し、Flashコンテンツの実行可能な代替手段として機能します。また、主要なブラウザーの提供元は、これらのオープンスタンダードをブラウザーに組み込み、他のほとんどのプラグイン（Adobe Flash Playerなど）を廃止しています。2017年にこのビジネス上の決定を発表し、3年間の猶予を設けることで、デベロッパー、デザイナー、事業者、その他の関係者が、必要に応じて既存のFlashコンテンツを新しいオープンスタンダードに移行するための十分な時間を確保できると考えました。