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。

●ルータ、エレベーターなど2億台のデバイスに影響を及ぼす脆弱性「URGENT/11」

https://monoist.atmarkit.co.jp/mn/articles/1907/30/news047.html
https://nakedsecurity.sophos.com/ja/2019/07/31/urgent-11-flaws-affect-200million-devices-from-routers-to-elevators/

このニュースをザックリ言うと・・・

- 7月29日（現地時間）、IoTセキュリティベンダーの米Armis社より、組み込み機器向けOSの「VxWorks」に未修正の脆弱性が存在すると発表されました。

- VxWorksは、工場・エレベーター・産業機器や医療機器の制御システムから、ファイアウォール・ルータ・VoIP電話・プリンタ等のネットワーク機器まで、20億以上のデバイスに搭載されていると言われるRTOS（リアルタイムOS）です。

- 脆弱性はCVE-2019-12255 ～ CVE-2019-12265の11個発見されたことから「URGENT/11」と呼ばれており、バージョン6.5以降のVxWorksでTCP/IP通信機能に存在するとされ、影響を受ける機器は2億個以上に及ぶとされています。

- VxWorksの開発元であるWind River社では、Armis社と共同で問題に対応、6月には顧客に対し通知を行っており、既に修正パッチもリリースしているとのことです。

AUS便りからの所感等

- 現時点でURGENT/11を悪用した攻撃は確認されていないとのことですが、ネットワークカメラ等で大規模な感染拡散を引き起こした「Mirai」のようなマルウェアが発生する可能性は決して否定できず、例えば、エレベーター等を制御するOSへのマルウェア感染により、多くのビルにおいて連鎖的な機能停止が発生する恐れも考えられます。

- ともあれ、機器にインターネットから不特定多数がアクセス可能であったり、あるいは社内LAN上のクライアントPC等と想定外の相互通信が可能であったりしないよう、適切なネットワーク構成をとっているか確認すべきです。

- VxWorksのような一般的なユーザには認識されにくいRTOSのみならず、各種アプライアンスやいわゆるIoT機器に対しては、ファームウェアの更新等といった管理の目がクライアント・サーバPC程には行き届きにくいケースは往々にして有り得ますので、組織内で所有している全ての機器について、所在を把握し、ベンダーサポート等の情報収集を定期的に行い、ファームウェア等を常に最新のバージョンに保つことを心がけるようにしましょう。

MONOist

「VxWorks」にゼロデイ脆弱性、「URGENT/11」は2億個のデバイスに影響

2019年07月30日 06時30分 公開　[朴尚洙，MONOist]

印刷　通知　59　Share　B!　12

米国のIoTセキュリティベンダーであるアーミス（Armis）は2019年7月29日（現地時間）、ウインドリバー（Wind River Systems）のRTOS（リアルタイムOS）「VxWorks」のゼロデイ脆弱性を発見したと発表した。バージョン6.5以降のVxWorksで、IPnet（TCP/IP）スタックを用いるものが対象。ただし、航空機や機能安全など規格認証が求められる機器向けに設計された「VxWorks 653」や「VxWorks Cert Edition」は対象になっていない。

アーミスは、発見したゼロデイ脆弱性が11個あることから、これらをまとめて「URGENT/11」と呼称している。ウインドリバーはアーミスの報告を受けてから共同して問題に対処しており、2019年6月には顧客にURGENT/11について通知し、対応するためのパッチも既に発行している。VxWorksを搭載する機器を展開している企業や組織は、直ちにパッチを適用する必要がある。パッチなどの詳細は、Wind River Security Center内の「Security Alert」を参照のこと。なお、両社によれば、URGENT/11を悪用した攻撃は確認されていないという。

naked security by SOPHOS

ルーター、エレベーターなど2億台のデバイスに影響を及ぼす脆弱性「URGENT/11」

31 JUL 2019　0

IoT, Security threats, Vulnerability

問題が存在しているのは、VxWorks の TCP/IP スタック（IPnet）です。これは、1987 年に導入されたソフトウェアスタックの一部であり、これまで脆弱性はほとんど発見されていませんでした。

リアルタイム

そもそも、RTOS とは何でしょうか。RTOS は、高速応答を保証する必要があり、処理能力よりも信頼性が重視されるデバイスで使用されます。

たとえば、自動車のエアバッグシステムは最適なタイミングで膨らまなくてはならないため（早すぎても遅すぎてもいけないため）、RTOS が使用されています。

加えて、32 年もの歴史があることから、Wind River の VxWorks は現在 2 億台のデバイスで使用されています。

●日本年金機構をかたるフィッシングに注意喚起

https://blog.kaspersky.co.jp/jp-nenkin-phishing/23924/

このニュースをザックリ言うと・・・

- 8月19日（日本時間）、日本年金機構より、同機構をかたるフィッシングメールが確認されているとして注意喚起が出されています。

- 例に示されているフィッシングメールは、件名が「［日本年金機構］個人年金電子ファイル情報更新。」で、本文は同機構のロゴが表示されるHTMLメールとなっており、またアンチウイルスベンダーのカスペルスキー社の記事によれば、リンク先では基礎年金番号を含む個人情報、さらにはクレジットカード情報をも詐取しようとしていた模様です。

- 8月22日現在、注意喚起で示されていたフィッシングサイトはChromeおよびFirefoxのアンチフィッシング機能によりアクセス時に警告が出るようになっており、ページ自体も表示されなくなっています。

AUS便りからの所感等

- カスペルスキー社の分析によれば、フィッシングサイトは正規のページに見せかけるために「電子政府の総合窓口(e-Gov)」サイトの一部ページのデザインを元にしていた一方、スクリプトのコメント部分や閉鎖状態のエラーメッセージは中国語になっていることから、中国の攻撃者が関与している（あるいはそう見せかけている）可能性が高いようです。

- フィッシングの回避策として、不審なメールやSMSが届いた場合は同様の報告がないかネット上の情報を確認すること、上記のようなブラウザやアンチウイルス・UTL等に備わっているアンチフィッシング機能を有効にすることが重要であり、加えて、通常使用するサービスへはメール上のリンクを安易にクリックせずブックマークからアクセスすることも推奨致します。


kaspersky daily

日本年金機構をかたるフィッシング

2019年8月26日

2019年8月、日本年金機構より「［日本年金機構］個人年金電子ファイル情報更新。」という不審なメールについて注意喚起が出されました。これは、日本年金機構をかたるフィッシングサイトへ誘導し、個人情報やクレジットカード情報の入力を求めるフィッシングメールに関するものです。

※この先は、分析のためにフィッシングサイトへのアクセスや情報の入力などの操作を行いますが、読者の皆様はそうした操作を行わないでください。

フィッシングサイトの概要

日本年金機構をかたるフィッシングサイトは、正規サイトとよく似たドメインを持っています。

正規サイト：nenkin.go.jp
フィッシングサイト：nenkins[.]com

この「nenkins[.]com」は2019年8月12日にドメイン登録されており、本稿執筆時点のIPアドレスは「167.179.82[.]250」でした。IPアドレスから地理情報を確認すると、米国のサーバー上に設置されていることが分かりました。

●流出パスワードの使用を警告するGoogleのChrome拡張、ユーザの1.5%に警告

https://www.itmedia.co.jp/news/articles/1908/16/news066.html

このニュースをザックリ言うと・・・

- 8月15日（現地時間）、Googleより、同社が2月に公開したChrome向けセキュリティ拡張「Password Checkup」による調査結果が発表されました。

- Password Checkupは、流出が確認された約40億件のユーザ名・パスワードを使ってログインしようとした際に警告を出すもので、調査はリリースから1ヶ月間にこれを使用した約67万人のChromeユーザに対して行っています。

- 約2,100万件のユーザ名・パスワードに対してスキャンを行い、1.5%に対して警告を出したとしており、またそのうちパスワードが変更されたのは26%程度だったのことです。

AUS便りからの所感等

- 上記とは別に、CNET Japanが7月に10～30代のスマホユーザに対して行ったアンケートでは、半数以上が「ID・パスワードに同じ文字列を使い回している」と回答したとの結果が出ており、リスト型攻撃による連鎖的な不正ログインの発生が問題となっている現状でも、対策が十分に根付いていない現状が窺えます。

- 複数のサイトでパスワードを使い回すことは、そのうちの一つでパスワードの流出が発生した場合、他のサイトについてもたちどころに不正ログインのターゲットとなることにつながり、結局はそれら全てのサイトにおいてもパスワードを変更しなければならなくなります。

- ともあれ、今日におけるパスワードの鉄則として「推測されにくい文字列にする」「サイト毎に別々の文字列にする」「覚えにくい場合は紙のメモあるいは管理ツール等を用いることも検討する」そして「流出が発覚したら速やかに変更する」ことを常に意識して頂ければ幸いです。


ITmedia NEWS

「Password Checkup」ユーザーの1.5%は流出パスワードを利用――Google調べ

[ITmedia]

米Googleは8月15日（現地時間）、2月に公開したセキュリティ拡張機能「Password Checkup」に関する調査結果と同拡張機能の新機能を発表した。

Password Checkupは、安全ではないユーザー名とパスワードに対して警告を表示するChromeブラウザ向けの拡張機能。ユーザーがChromeで何らかのサービスにログインする際、Googleが把握している、約40億件の流出したユーザー名とパスワードとログイン情報を照らし合わせ、合致すると警告を表示する。