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。

●NTT東西「ひかり電話ルータ／ホームゲートウェイ」に脆弱性、最新ファームへ更新を

https://internet.watch.impress.co.jp/docs/news/1192906.html
https://web116.jp/ced/support/news/contents/2019/20190626.html

このニュースをザックリ言うと･･･

- 6月26日（日本時間）、IPAおよびJPCERT/CCより、NTT東日本・西日本各社の「ひかり電話」契約者に配布されている「ひかり電話ルータ／ホームゲートウェイ」にクロスサイトスクリプティング（XSS）とクロスサイトリクエストフォージェリ（CSRF）の脆弱性が存在するとして注意喚起が出されています。

- 脆弱性の悪用により、当該機器の管理画面上で、攻撃者が指定したスクリプトを実行されたり偽のフォームを表示されたりする（XSS）、あるいは機器に対する不正な設定を強制的に実行される（CSRF）可能性があります。

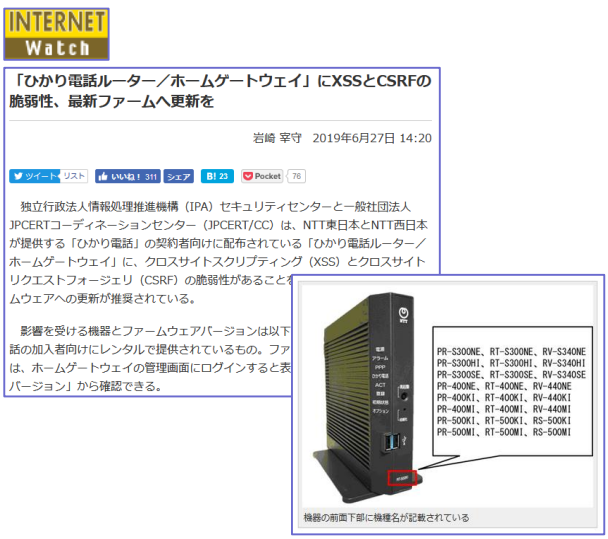
- IPA・JPCERT/CC・NTT各社では脆弱性が存在する機種・ファームウェアのバージョン情報およびその確認・アップデート方法を公開しており、該当する場合はアップデートするよう呼び掛けています。

AUS便りからの所感等

- XSSやCSRFといった脆弱性はWebアプリケーション側において適切な対策を行っていない場合に発生するものですが、一般的なWebサイトのみならず、メーカー製のネットワーク機器におけるWebベースの管理画面でも時折報告され、特にその場合はファームウェアが確実に更新されるケースが少なく、脆弱性が放置される傾向にあります。

- 当該機器の管理画面へは、通常IPアドレスではない固有のドメイン名のURLでアクセス可能であることから、攻撃者側は相手の機器のプライベートIPアドレス情報を取得する必要なしに、脆弱性を突こうとする罠サイトを設置したり、不正なURLを含んだメールを拡散させたりすることが可能であることに注意が必要です。

- 管理画面へのログイン権限を持つユーザにおいては、ファームウェア更新までの回避策として、かつ普段から脆弱性を悪用した攻撃に誘導される可能性を抑えるため、「管理画面へはプライベートモード(シークレットウィンドウ)を使ってログインする」あるいは「管理画面へのログインとWebメールの閲覧をはじめとした他のWebサイトへのアクセスとは同じブラウザ上で同時に行わない」ことを推奨致します。


INTERNET Watch

「ひかり電話ルーター／ホームゲートウェイ」にXSSとCSRFの脆弱性、最新ファームへ更新を

岩崎 宰守　2019年6月27日 14:20

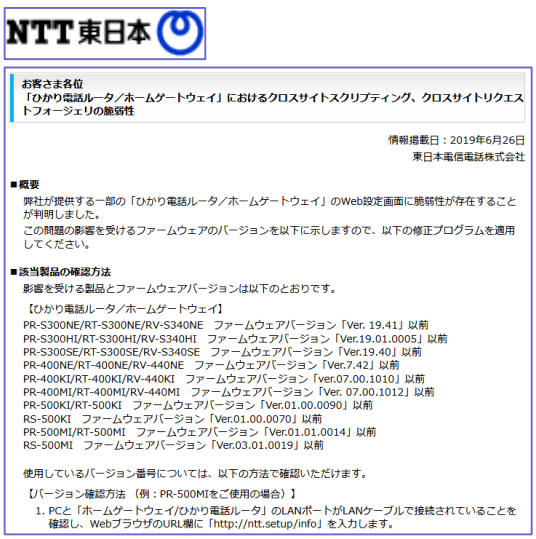
ツイート リスト　いいね！ 311　シェア　B! 23　Pocket 76

独立行政法人情報処理推進機構（IPA）セキュリティセンターと一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、NTT東日本とNTT西日本が提供する「ひかり電話」の契約者向けに配布されている「ひかり電話ルーター／ホームゲートウェイ」に、クロスサイトスクリプティング（XSS）とクロスサイトリクエストフォージェリ（CSRF）の脆弱性があること[illegible]ムウェアへの更新が推奨されている。

影響を受ける機器とファームウェアバージョンは以下話の加入者向けにレンタルで提供されているもの。ファは、ホームゲートウェイの管理画面にログインすると表バージョン」から確認できる。

PR-S300NE、RT-S300NE、RV-S340NE
PR-S300HI、RT-S300HI、RV-S340HI
PR-S300SE、RT-S300SE、RV-S340SE
PR-400NE、RT-400NE、RV-440NE
PR-400KI、RT-400KI、RV-440KI
PR-400MI、RT-400MI、RV-440MI
PR-500KI、RT-500KI、RS-500KI
PR-500MI、RT-500MI、RS-500MI

機器の前面下部に機種名が記載されている


NTT東日本

お客さま各位
「ひかり電話ルータ／ホームゲートウェイ」におけるクロスサイトスクリプティング、クロスサイトリクエストフォージェリの脆弱性

情報掲載日：2019年6月26日
東日本電信電話株式会社

■概要
弊社が提供する一部の「ひかり電話ルータ／ホームゲートウェイ」のWeb設定画面に脆弱性が存在することが判明しました。
この問題の影響を受けるファームウェアのバージョンを以下に示しますので、以下の修正プログラムを適用してください。

■該当製品の確認方法
影響を受ける製品とファームウェアバージョンは以下のとおりです。

【ひかり電話ルータ／ホームゲートウェイ】
PR-S300NE/RT-S300NE/RV-S340NE　ファームウェアバージョン「Ver. 19.41」以前
PR-S300HI/RT-S300HI/RV-S340HI　ファームウェアバージョン「Ver.19.01.0005」以前
PR-S300SE/RT-S300SE/RV-S340SE　ファームウェアバージョン「Ver.19.40」以前
PR-400NE/RT-400NE/RV-440NE　ファームウェアバージョン「Ver.7.42」以前
PR-400KI/RT-400KI/RV-440KI　ファームウェアバージョン「ver.07.00.1010」以前
PR-400MI/RT-400MI/RV-440MI　ファームウェアバージョン「Ver. 07.00.1012」以前
PR-500KI/RT-500KI　ファームウェアバージョン「Ver.01.00.0090」以前
RS-500KI　ファームウェアバージョン「Ver.01.00.0070」以前
PR-500MI/RT-500MI　ファームウェアバージョン「Ver.01.01.0014」以前
RS-500MI　ファームウェアバージョン「Ver.03.01.0019」以前

使用しているバージョン番号については、以下の方法で確認いただけます。

【バージョン確認方法　（例：PR-500MIをご使用の場合）】
1. PCと「ホームゲートウェイ/ひかり電話ルータ」のLANポートがLANケーブルで接続されていることを確認し、Webブラウザ[illegible]URL欄に「http://ntt.setup/info」を入力します。

●東京五輪便乗の攻撃に注意…公式サイトの類似ドメイン名、チケット抽選結果をかたる偽メール等

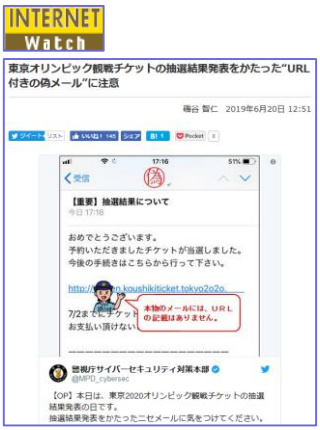
https://internet.watch.impress.co.jp/docs/news/1191500.html

このニュースをザックリ言うと・・・

- 5月30日（日本時間）、早稲田大学の森達哉研究室より、東京五輪公式サイト（tokyo2020.org）に類似したドメイン名が956件取得されており、一部はマルウェア感染等の可能性がある不正なサイトと判定されていたとする調査結果が発表されています。

- また観戦チケットの抽選に関しては、抽選結果発表が行われた6月20日、警視庁サイバーセキュリティ対策本部より、抽選結果発表をかたる偽メールへの注意喚起が出されており、「当選おめでとう。手続きは以下のURLから行って下さい」といった文とともにリンクが貼られているようなメールは全て偽物であると呼びかけられました。

AUS便りからの所感等



- 今回のオリンピックに便乗した攻撃は、例えば2018年9月にも偽メールからマルウェアに感染させようとする攻撃が確認されており（AUS便り 2018/09/10号参照）、こういった攻撃への対策のためか、チケット申込み〆切日の5月29日の時点で「結果メールにはリンクやURLは記載しない」とし、抽選結果は必ず公式販売サイトにアクセスして行うよう呼びかけられていました。

- 類似ドメイン名について、ニュース等でも「本物のドメイン名か確認すること」がよく挙げられていますが、人間の目だけで確実に確認することは困難であり、アンチウイルスやブラウザ、メーラーおよびUTM等のセキュリティ機能を活用するに越したことはありません。

- チケット購入手続の期限となる7月2日以降にも、例えば「チケットの二次募集が行われる」等と題してフィッシングメールが拡散する可能性も考えられ、今後も公式に出されている情報の事前確認と、不審なメールに対するSNS等での報告に常時目を向けることが重要です。

●NASA、サイバー攻撃で機密データ流出…侵入口は無許可接続の「Raspberry Pi」

https://www.itmedia.co.jp/news/articles/1906/23/news012.html

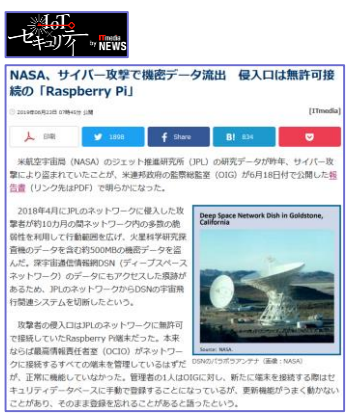
このニュースをザックリ言うと・・・

- 6月18日（現地時間）、米連邦政府監察総監室（OIG）より、米航空宇宙局（NASA）ジェット推進研究所（JPL）がサイバー攻撃を受け、研究データを盗まれていたことが発表されました。

- 発表によれば、攻撃者は2018年4月にJPLのネットワークに侵入、以後約10ヶ月間、ネットワーク内の多数の脆弱性を突きながら、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ可能性があるとしています。

- ネットワークには本来承認された機器だけが接続を許可されていましたが、小型PC「Raspberry Pi」が無許可で接続され、それが侵入口とされたとのことです。

AUS便りからの所感等



- Raspberry Piは、クレジットカード程度のサイズながらも、有線LAN（一部機種はWi-Fiも）やUSB等のポートを備え、Linux等を動かすのに必要十分な性能を持ち、かつ安価（5～55ドル）であることから、研究開発やサーバ・ルータとしての運用等、業務用途でも用いられる程の人気があります。

- 当該機器が設置された経緯や、ネットワークに接続されている機器を自動的に検知・管理するシステムが導入されていたかは不明ですが、少なくとも身元不明な機器が接続できないような仕組みにはなっていなかったと推測されます。

- 今日、BYOD（個人が所有する機器の業務利用）を認めるケースも珍しくはなくなっていますが、悪意のある機器、あるいは管理が行き届いておらず攻撃の格好のターゲットとなり得る機器等の存在を確実に把握し、承認した機器のみがネットワークに接続できるようなソリューションの導入が安全なネットワークの運用のためには肝要です。