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東日本のHGW・ひかり電話ルータに脆弱性…機種、ファームウェアバージョン確認を

https://internet.watch.impress.co.jp/docs/news/1626046.html
https://jvn.jp/jp/JVN78356367/index.html
https://web116.jp/ced/support/version/

このニュースをザックリ言うと･･･

- 9月24日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、NTT東日本が提供する複数のホームゲートウェイ(HGW)・ひかり電話ルータに脆弱性(CVE-2024-47044)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、「WAN側から当該製品の設定画面にアクセスされる」可能性があるとされています。

- 該当する機種はRT-400MI・PR-400MI・RV-440MI・PR-500MI・RS-500MI・RT-500MI・PR-600MI・RX-600MIで、7月29日から8月26日にかけてファームウェアのアップデートがリリースされています。

AUS便りからの所感等

- JVNに掲載された情報によれば、脆弱性の影響を受けるのはNTT東日本エリアで契約している場合に限られ、かつ攻撃者が機器のWAN側IPv6アドレスを特定する必要があるとしています。

- 管理画面へのログイン自体はさらにパスワードの入力が必要とみられるとはいえ、LAN側からのみアクセス・ログインが可能であるという前提が破れるということが問題と言えます。

- 多くの機器ではデフォルトでファームウェアの自動更新を行うよう設定されており、現時点では更新済みのはずですが、機器の管理者においては、もし手動で行うよう設定を変更していた場合に必ず速やかに更新を実施するとともに、設定に拘らず可能な限り実際に更新されているか確認することを推奨致します。

- さらには機種が今回の発表に該当していなかったとしても、NTT東日本(および西日本)が提供するファームウェアのバージョンアップ情報に目を通し、使用している機器のファームウェアが最新か確認する体制をとることが重要です。

Impress Watch

NTT東日本が提供する「RT-400MI」など複数のホームゲートウェイ／ひかり電話ルーターに、アクセス制限不備の脆弱性。最新ファームウェアへの更新を

大竹 莉子　2024年9月25日 12:15

RT-400MI（NTT東日本のウェブサイトより）

東日本電信電話株式会社（NTT東日本）が提供する複数のホームゲートウェイ／ひかり電話ルーターに、アクセス制限不備の脆弱性が存在するとして、脆弱性対策情報ポータルサイト「JVN（Japan Vulnerability Notes）」が9月24日に情報を公開した。対策のため、ファームウェアを最新バージョンに更新するよう呼び掛けている。

当該の脆弱性のCVEレコードはCVE-2024-47044で、CVSS v3のスコアは5.3。当該製品のWAN側IPv6アドレスを特定した攻撃者によって、WAN側から当該製品の設定画面にアクセスされる可能性がある。

●ディスプレイからノイズ音を発生、エアギャップを通して情報を奪取する手口「PIXHELL」

https://news.mynavi.jp/techplus/article/20240912-3023125/
https://www.itmedia.co.jp/news/articles/2409/17/news052.html
https://thehackernews.com/2024/09/new-pixhell-attack-exploits-screen.html
https://arxiv.org/abs/2409.04930

このニュースをザックリ言うと・・・

- 9月10日(現地時間)、「The Hacker News」にて、イスラエルのセキュリティ研究者が発表した、エアギャップ(ネットワークに接続されていない)状態のPCから情報を奪取する攻撃手法が取り上げられています。

- 「PIXHELL」と名付けられたこの手法では、PCに接続されたディスプレイ上で映像が表示される際にディスプレイから生じるノイズ音(いわゆるコイル鳴き)を用いて情報を外部に流出させるもので、流出させるデータの内容に応じたピクセルパターンを表示して0～22kHzの周波数のノイズ音を発生するとしています。

- ただし攻撃の実行には、ターゲットとなるディスプレイの機種に合わせたピクセルパターンを用意し、ノイズ音を聞き取ってデータを入手するため近くにマイクやスマートフォンを設置する必要があるとし、また不審な映像の表示や人間の可聴域でのノイズ音の生成で攻撃に気付かれる可能性はあるとされています。

AUS便りからの所感

- ディスプレイのみならずキーボード・マウスおよびそれらを接続するケーブルから生じる電磁波を分析して情報を読み取る「テンペスト攻撃」等が、2000年代の時点で問題視されています。

- 前述した準備以外にも、エアギャップ状態のPC上でピクセルパターンを表示させるために、別途マルウェア感染等の侵入を行う必要があるとみられますが、一見成功しづらいと思われる手法こそ成立し得る可能性があると心得、LAN等に接続されていないPCであってもUSBメモリー等からのマルウェア感染の恐れに対しアンチウイルス等による防御を確実に行うことは肝要と言えます。


TECH Powered by マイナビニュース

液晶ディスプレイをスピーカーにしてデータを盗む方法が見つかる

掲載日 2024/09/12 08:43　　著者：後藤大地

The Hacker Newsは9月10日(現地時間)、「New PIXHELL Attack Exploits Screen Noise to Exfiltrates Data from Air-Gapped Computers」において、スピーカーなどのオーディオデバイスを接続していないエアギャップネットワーク(物理的に隔離されたネットワーク空間)上のコンピュータから音響信号を作り出して情報を窃取する「PIXHELL」と呼ばれる攻撃手法が開発されたと伝えた。

ネゲヴ・ペン＝グリオン大学のMordechai Guri博士により開発されたPIXHELLの論文は、「[2409.04930] PIXHELL Attack: Leaking Sensitive Information from Air-Gap Computers via 'Singing Pixels'」から閲覧することができる。

● 8月度フィッシング報告は166,556件、フィッシングサイト件数は過去最多

https://www.antiphishing.jp/report/monthly/202408.html

このニュースをザックリ言うと・・・

- 9月19日(日本時間)、フィッシング対策協議会より、8月に寄せられたフィッシング報告状況が発表されました。

- 8月度の報告件数は166,556件で、7月度(https://www.antiphishing.jp/report/monthly/202407.html)の177,855件からは11,288件減少しています。

- フィッシングサイトのURL件数は85,768件で7月度(38,591件)から47,177件増加、悪用されたブランド件数は68件で7月度(73件)から5件減少となっています。

- Amazonを騙るフィッシングが全体の約20.2%を占め、次いで20,000件以上の報告を受けたイオンカード、ヤマト運輸、東京電力と合わせて約62.7%、さらに1,000件以上報告された16ブランドまで含めると約89.9%を占めたとのことです。

- スミッシング(SMSによるフィッシング)は東京電力を騙るものが多かった一方、これまで多かった宅配便を騙るものが減少しているとのことです。

AUS便りからの所感

- フィッシングサイトURL件数が急増したことについて、大量メール配信を行うタイプのフィッシングでサブドメインにランダム文字列を使ったURLへの誘導が多かったためと分析しています(なお使用されるトップレベルドメイン名は.cnと.comのものが依然突出しています)。

- 調査用メールアドレスに届いたフィッシングメールにおけるなりすましの割合は2月の約22.8%から上昇、5～7月に50%台だったものが8月には急増して約77.1%となっている一方、DMARC(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)のポリシーがreject(受信拒否)またはquarantine(迷惑メールフォルダー等への隔離)となっているものも約63.5%となり、DMARCによるチェックでフィルタリングを行えるケースが多くなっているとのことで、メールサーバー管理者においては取引相手等を保護するべく、各種フィッシング対策機構を有効にするのはもちろん、導入の初期段階で緩いポリシーとしていたものについても、着実な検証の上で厳しいものに設定していくことを検討すべきでしょう。


フィッシング対策協議会
Council of Anti-Phishing Japan