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。

●米大統領公式サイト等に重大な欠陥、「デバッグモード」で放置

https://forbesjapan.com/articles/detail/30272
https://www.comparitech.com/blog/vpn-privacy/debug-mode-exposes-credentials/

このニュースをザックリ言うと･･･

- 10月17日(現地時間)、IT関係のレビュー・比較を行う英Comparitech社より、米トランプ大統領の公式サイト等少なくとも768のWebサイトに脆弱性を確認したと同社ブログで発表されました。

- 脆弱性はこれらのWebサイトで使用しているソフトウェア「Laravel」の「デバッグモード」によるもので、デバッグモードが有効な設定のまま運用されていたことにより、サイトのデータベースのロケーションやパスワード、暗号キー等のセンシティブな情報が露呈していたとのことです。

- 同社では同11日大統領公式サイトの運営に報告し、5日後に問題は解決済みとの返答を受けたとしています。

AUS便りからの所感等

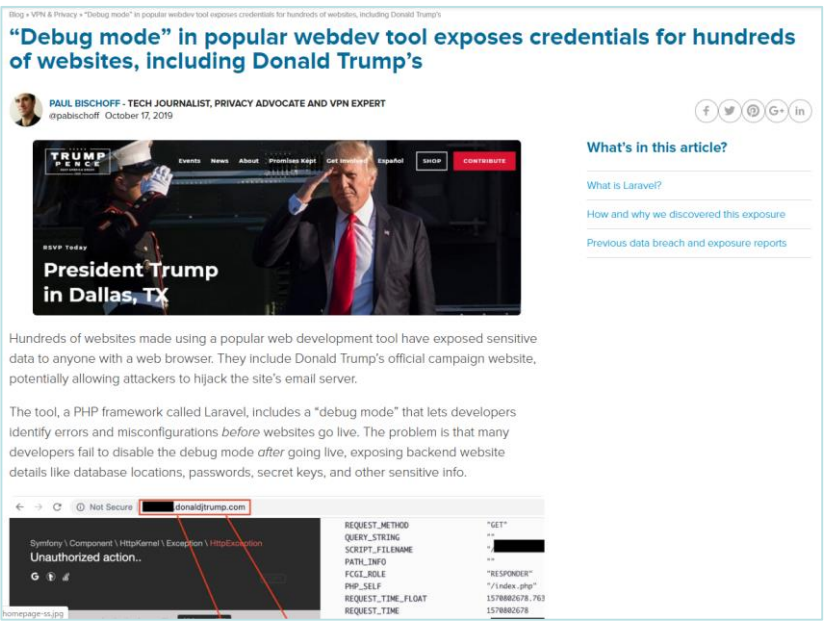
- LaravelはPHPによるWebサイト構築を行うためのいわゆる「Webアプリケーションフレームワーク」の一つで、近年非常に高い人気を得ています。

- デバッグモードが有効になっている場合、Webアプリケーションからのエラーメッセージ以外にも広範囲な情報をブラウザー上で見ることが可能となり、攻撃者にとっては様々な攻撃を行うための手掛かりとなる恐れがあります。

- このようなデバッグモードは開発時の環境でのみ有効とし、不特定多数のユーザーが閲覧する本番環境ではこれを無効にすることや、テスト用のページ・バックアップファイル等をアクセス可能な状態で残さないよう削除する等の対策をとること、また不必要な情報の露呈がないか可能な限り第三者機関の診断を受けることが肝要です。

Forbes JAPAN

comparitech



●ホテルの客室ロボットに乗っ取り・盗撮の可能性…宿泊客が指摘

https://www.itmedia.co.jp/news/articles/1910/17/news131.html
https://www.itmedia.co.jp/news/articles/1910/18/news119.html
https://www.hennnahotel.com/maihama/news/1403/
https://mjirobotics.co.jp/191018-2/

このニュースをザックリ言うと・・・

- 10月17日(日本時間)、H.I.S.ホテルホールディングス社(以下H.I.S.ホテル)より、同社が運営する「変なホテル舞浜 東京ベイ」の客室に設置していたコミュニケーションロボット「Tapia」に乗っ取りが可能な脆弱性が指摘されていたことが発表されました。

- 脆弱性の悪用により、プログラムが書き換えられ、他の客の映像や音声を取得してリモートから視聴することが可能であったとされ、同社では全客室のTapiaについて不正なアプリケーション等のインストールがされていなかったことを確認するとともに、不正アクセスの対策を行ったとしています。

- 翌18日には、開発元のMJI社からも、脆弱性が存在すること、不正アプリ検知・削除機能を配信予定であることが発表されています。

AUS便りからの所感

- ホテルの宿泊客とみられる人物が同12日にTwitterに脆弱性の存在を指摘する投稿を行ったことが今回の発表のきっかけとされています(その約90日前には同社に直接メールで指摘を行ったとのことです)。

- 脆弱性はインターネット上からではなく、攻撃者がロボットの近くからNFCを経由して突くものだったとされていますが、機能が多ければ多いほどそれぞれが攻撃者の侵入経路となり得るものと心得、また一般的なネットワーク通信以外にも物理的な経路からの攻撃にも注意を怠らず安全性を確保することが、こと今回のロボットのような「IoT機器」では重要となることでしょう。

●遠隔操作可能なLightningケーブルの可能性、Sophosが注意喚起

https://news.mynavi.jp/article/20191021-cablehack/
https://nakedsecurity.sophos.com/2019/10/02/omg-evil-lightning-cable-hits-prime-time/

このニュースをザックリ言うと・・・

- 10月2日(現地時間)、セキュリティベンダーの英Sophos社より、遠隔操作可能なLightningケーブルが出回る可能性があると同社ブログで注意喚起が出されています。

- ブログ記事で紹介されている「O.MG Cable」は、一見普通のLightningケーブルに見えるものの、Wi-Fiアクセスポイントあるいはクライアントの機能を持つ小型モジュールが組み込まれており、接続したPCをリモートから乗っ取ること等が可能になるとしています。

- 記事では、同様の仕掛けがされたUSBケーブルも2月に開発されていたとしており、対策として「カフェなどの公衆の場所で、バックやコンピュータを置きっ放しにして離席しない」「ケーブルを安全にし、すぐに見分けがつくように印をつける等を行う」「人からケーブルや充電器を借りる時は十分注意する」等を挙げています。

AUS便りからの所感等

- 不審なモバイルデバイスを接続する問題への指摘としては、2015年に、USB機器のファームウェアに不正なプログラムを仕込む「BadUSB」攻撃、あるいは約300個のUSBメモリを放置したところ約半数が拾ってPCに接続したとする実験結果が発表されています。

- さらに2014年には、USBから給電可能な電子タバコをPCに接続したところマルウェアに感染した、というケースも報告されています。

- 一般的なモバイルデバイスからの攻撃の可能性に対しては、「USBメモリやDVD-ROM等から何らかのプログラムを自動実行させないよう可能な限り設定を行う」「アンチウイルスによるUSBメモリのスキャンおよびPCへの感染防御を確実に行う」等を可能な限り行うべきですが、今回のケースを含めた究極的な対策となると、全てのUSBデバイスはもちろん、それに接続するケーブルをも資産管理の対象とすること等も必要になってくるものと思われます。