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。

●原発処理水放出への抗議か…ルーター機器へ不正アクセス、管理画面改ざんの被害

https://www.asahi.com/articles/ASR8Y61XZR8YULZU00C.html
https://www.lac.co.jp/lacwatch/alert/20230831_003494.html
https://www.seiko-sol.co.jp/archives/78347/

このニュースをザックリ言うと･･･

- 8月29日(日本時間)、朝日新聞より、セイコーソリューションズ(以下・SSOL)社製ルーター機器少なくとも約1,500台が不正アクセスを受け、管理画面が改ざんされる被害が発生していると報じられています。

- 同日のSSOL社からの注意喚起によれば、対象となっている機器はSkyBridge MB-A100・MB-A110・MB-A200、SkyBridge BASIC MB-A130およびSkySpider MB-R210で、2月28日に発表・セキュリティアップデート提供済みの脆弱性を悪用したものとされています。

- 改ざんされた画面には「海は人類共通の財産です」「日本政府は独自路線を貫き、全人類に対する罪である核下水を排出している」というメッセージが表示されるようになっており、8月24日に始まった東京電力福島第一原発の処理水放出に抗議する内容とみられています。

- 8月31日には国内情報セキュリティ大手のラック社からも注意喚起が出ています。

AUS便りからの所感等

- 改ざんを行った攻撃者とみられるSNSアカウントが、攻撃手法や脆弱な機器を検索する方法を挙げ、「これは私たちの最初の警告である」とさらなる攻撃を示唆する投稿を行っていたとされており、また管理画面のアカウント情報が奪取されネット上に掲載されていたという情報もあります。

- 今回の攻撃による改ざんはあくまで管理画面の表示に留まっていたようですが、その他のルーターの設定変更を行うことも可能な状況だったとみられ、今後さらなる攻撃の発生時には当然そういったレベルに立ち入られる恐れも十分に考えられます。

- ルーターやIoT機器の脆弱性は他のメーカーにおいても度々報告されており、攻撃者はあらゆる機器の脆弱性情報をもとに日々アップデートを行っていない機器を検索し、攻撃あるいはその準備を行っていると考えられるため、外部ネットワークから管理画面等にアクセス可能な状態にある物を含めあらゆるIoT機器・ネットワーク機器についてファームウェアを最新バージョンに保ち、またアップデートの提供が終了している機器は確実にリプレースする管理体制をとることが重要です。

朝日新聞 DIGITAL

「全人類に対する罪　核下水排出」 日本のルーターが画面改ざん被害

編集委員・須藤龍也　2023年8月29日 19時00分

ハッキングを受け改ざんされた画面

日本にあるインターネットの ルーター 機器がハッキングされ、東京電力福島第一原発 の 処理水 放出に抗議する内容のメッセージが表示されるよう、画面が改ざんされる被害が起きていることがわかった。サイバー攻撃 を受けたとみられる。

この機器は、セイコー ソリューションズ（千葉市）が発売する「SkyBridge」と「SkySpider」。ハッキングを受けると、機器の内部にアクセスする際の認証画面が改ざんされ、「日本政府は独自路線を貫き、全人類に対する罪である核下水を排出している」などのメッセージが表示される。

同社によると、28日夕に被害を把握し、台数などは調査中という。記者が確認したところ、29日午前の段階で少なくとも約1500台の機器の被害が確認された。

●VBSマクロ実行、PDFファイルとして検知回避…新たな攻撃手法「MalDoc in PDF」に注意喚起

https://forest.watch.impress.co.jp/docs/news/1525553.html
https://blogs.jpcert.or.jp/ja/2023/08/maldocinpdf.html

このニュースをザックリ言うと･･･

- 8月22日(日本時間)、JPCERT/CCより、7月に発生した攻撃で利用された不正な文書データ形式についての解説と注意喚起が出されています。

- 「MalDoc in PDF」と名付けられた文書データは、PDF形式のファイルヘッダーの後ろに、Wordで実行される不正なVBSマクロ(厳密にはMHTML形式のデータ)を埋め込んだものとされています。

- 拡張子が「.doc」のものが確認されており、ファイルを開いた際にWordで処理され、VBSマクロが実行されることが意図されている一方、アンチウイルスでの解析時にはPDFとして検知され、またPDFビューアーで開いた場合にはスクリプト等が実行されないような形になっていることから、不正なファイルとしての検出を回避されやすい可能性があるとのことです。

AUS便りからの所感

- 類似した攻撃手法としては、Webアプリケーションにおけるクロスサイトスクリプティング(XSS)の一種として、HTMLではないテキストファイルや画像ファイル等に不正なスクリプトが実行されるようなHTMLのタグを埋め込み、ブラウザー上でこれをHTMLデータとして開くよう誘導するものも用いられていました。

- 解説では自動的なマルウェアチェックで当該ファイルがPDFとして扱われた場合に不正なファイルとして判定されない可能性について注意するよう呼び掛けている一方、悪性なWordファイル専用の分析ツールや、データに特定の文字列が含まれるかチェックする等により、不正なVBSマクロの検出は可能であるとしています。

- 各種アンチウイルス・UTM製品において、今後この攻撃手法が周知されることにより、適切に検出されるようになるものと期待されますが、手元のアンチウイルス等で反映されるようになるには、常時エンジンやパターンファイル等が最新バージョンに更新される状態である必要があることにも注意してください。

Impress Watch

多くのセキュリティツールをすり抜ける新攻撃手法「MalDoc in PDF」 ～JPCERT/CCが警告

7月に発生したセキュリティ攻撃で実際に用いられる

樽井 秀人　2023年8月23日 12:29

一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は8月22日、公式ブログ「JPCERT/CC Eyes」で、セキュリティソフトの検出を回避する新たな手法「MalDoc in PDF」を確認したと発表した。7月に発生したセキュリティ攻撃で用いられていたという。

「MalDoc in PDF」は、「Microsoft Word」で作成されたマクロ付きのMHTMLデータをPDFファイルへ埋め込む点が特徴。作成されたファイルはシステムから見るとPDFファイルだが、「Word」で開くこともできる。その場合、ファイルに埋め込まれた悪意あるVBSマクロが実行されてしまう可能性がある。

●8月はWordPressの21のプラグインに脆弱性…Sucuri社発表

https://news.mynavi.jp/techplus/article/20230903-2762478/
https://blog.sucuri.net/2023/08/wordpress-vulnerability-patch-roundup-august-2023.html

このニュースをザックリ言うと･･･

- 8月31日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、8月に報告された21のWordPressプラグインに存在する脆弱性のまとめ記事が発表されました。

- うち、フォーム設置用の「Forminator」で不正なファイルのアップデートが可能となる脆弱性と、eコマースプラグインWooCommerceへの機能拡張を行う「TI WooCommerce Wishlist」におけるSQLインジェクションの脆弱性が、特に危険なものである「緊急(Critical)」レベルの脆弱性とされています。

- 他にもクロスサイトスクリプティング(XSS)や機密情報漏洩等の脆弱性4件が、上記に次いで危険な「重要(High)」レベルとされています。

AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、毎月20件台の報告がまとめられています(7月には36件と通常より多く報告されています)。

- またWordPress本体においても不定期にセキュリティアップデートがリリースされるため、インストールした状態のままで放置するようなことは決してせず、随時本体・プラグインを最新に保つよう努めること、セキュリティを強化する何らかのプラグインを導入すること、並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFや、IDS・IPSの導入を検討することを強く推奨致します。

TECH Powered by

WordPressプラグイン21個に新たな脆弱性、確認とアップデートを

掲載日 2023/09/03 15:49　著者：後藤大地

Sucuriは8月31日(米国時間)、「WordPress Vulnerability & Patch Roundup August 2023」において、2023年8月に明らかになったWordPressの脆弱性およびセキュリティパッチの情報について伝えた。SucuriはWebサイト所有者に対して新たな脅威を把握して対処してもらえるよう、1カ月間のWordPressエコシステムの重要なセキュリティアップデートと脆弱性パッチの一覧をまとめて公表している。