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。

●「サポート詐欺」に関するレポート、IPA発表

https://www.ipa.go.jp/security/anshin/measures/supportscam_report.html

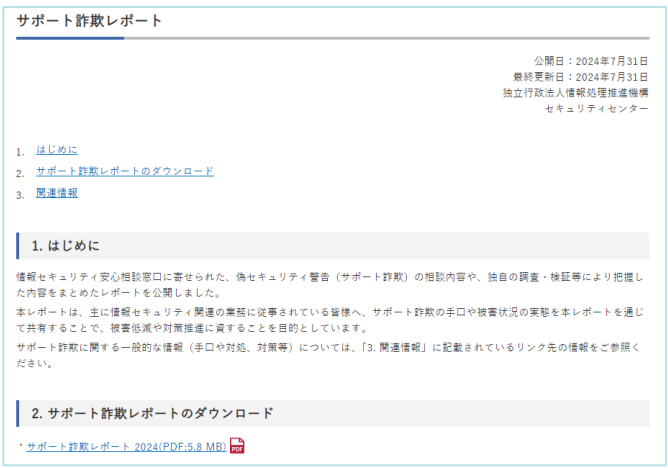
このニュースをザックリ言うと･･･

- 7月31日(日本時間)、IPAより、「サポート詐欺レポート 2024」が公開されました。
- いわゆる「サポート詐欺(偽セキュリティ警告)」について、これまで同組織の「情報セキュリティ安心相談窓口」に寄せられた相談内容や、独自の調査・検証等により把握した内容をまとめたレポートとのことです。
- IPAでは2023年12月に、現在特に問題となっている「ブラウザーが全画面表示となるケース」の偽セキュリティ警告画面を体験できるサイトを開設する等の施策をとっていましたが、今回のレポートでは以前から確認されていた手口を含め、より広範囲に豊富な画像を用いて紹介しています。

AUS便りからの所感等

- サポート詐欺の相談件数は、月間では2024年4月に過去最多の828件を記録、四半期でも近年は概ね右肩上がり傾向で、2024年4月～6月期にやはり最多の1,767件を記録しています。
- 「本手口の実際の流れにおける変化と特徴」の節では、以前から存在したような、ブラウザーの通知機能を悪用し、Windowsの通知領域から不審な表示を行うケース等から取り上げられています。
- 前述した体験サイトにおいても、強制的な全画面表示を解除する方法として「ESCキーの長押し」が挙げられていますが、2023年当初にブラウザーを強制終了させるための手順を複数案内していたところ、これらが効かなくなるケースが増えていたという経緯が述べられています(この他、ノートPCのスリープからの復帰に起因してごくまれに「ESCキーの長押し」が効かなくなる状況があり、これに遭遇した場合の回避策等も紹介されています)。
- 是非ともすべてのユーザーにおいて、サポート詐欺回避のため今回のレポートを熟読し、手口を把握した上で慎重に行動するよう努めることを推奨致します。

IPA 独立行政法人 情報処理推進機構


サポート詐欺レポート

公開日：2024年7月31日
最終更新日：2024年7月31日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに
2. サポート詐欺レポートのダウンロード
3. 関連情報

1. はじめに

情報セキュリティ安心相談窓口に寄せられた、偽セキュリティ警告（サポート詐欺）の相談内容や、独自の調査・検証等により把握した内容をまとめたレポートを公開しました。
本レポートは、主に情報セキュリティ関連の業務に従事されている皆様へ、サポート詐欺の手口や被害状況の実態を本レポートを通じて共有することで、被害低減や対策推進に資することを目的としています。
サポート詐欺に関する一般的な情報（手口や対処、対策等）については、「3. 関連情報」に記載されているリンク先の情報をご参照ください。

2. サポート詐欺レポートのダウンロード

・サポート詐欺レポート 2024(PDF:5.8 MB)

●DNSサーバー「BIND」に4件の脆弱性、DoS攻撃の可能性あり

https://news.mynavi.jp/techplus/article/20240725-2992472/
https://jvn.jp/vu/JVNVU99505181/
https://www.jpcert.or.jp/newsflash/2024072401.html
https://jprs.jp/tech/

このニュースをザックリ言うと･･･

－7月24日(日本時間)、DNSサーバー「BIND」に4件の脆弱性が発見されたとして、修正バージョン(9.18.28/9.20.0等)がリリースされました。

－脆弱性の悪用により、BINDのサーバープロセスを不正にダウンさせられる、あるいはBINDが動作しているサーバーのパフォーマンスを低下させられるといった、外部からのDoS攻撃に繋がり得るものとなっています。

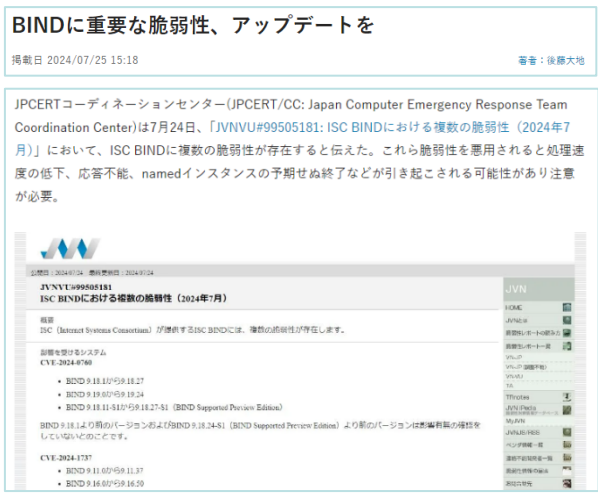
－JPRSやJPCERT/CC等からの注意喚起では、4件とも緊急性が高いとされており、可能な限り速やかなアップデートが推奨されています。

AUS便りからの所感

－BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあり、近年は殆どの脆弱性がサーバープロセスのダウンやパフォーマンス低下といったDoS攻撃に繋がるものとなっています。

－8/1現在での各Linuxディストリビューションにおけるアップデートのリリース状況はまちまちで、Debian・Ubuntuからはアップデートがリリースされている一方、RHELおよび派生ディストリビューション(Rocky Linux・Almalinux等)についてはまだリリースされていない模様です(後者はディストリビューション公式のもの以外に別途BIND開発元からもパッケージが提供されています)。

－代替として他のソフトウェアあるいはAWSのRoute53といったクラウドサービスを使用するケースも多くなっているものの、メーカー製ネットワーク機器においてBINDを組み込んでいるケース等にも影響し得ることを鑑み、使用しているソフトウェア・機器のファームウェアについて脆弱性の有無やアップデートのリリース状況を随時確認すること、リリースされ次第適用を行うことが肝要です。



●夏季休暇における情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20240801.html
https://www.ipa.go.jp/security/anshin/measures/vacation.html

このニュースをザックリ言うと･･･

－8月1日(日本時間)、IPAより、「夏休みにおける情報セキュリティに関する注意喚起」が発表されました。

－お盆の時期は企業・組織によっては多くの人が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

AUS便りからの所感

－IPAは毎年の夏季・冬季休暇およびゴールデンウィークの時期に注意喚起を行っていますが、休暇までに日にちがなく十分な対応が間に合わなかったとしても、お盆明け以降に点検すべきことは多く存在しますし、以後も年末年始・ゴールデンウィーク等に備えて対応しておくべき事柄も変りません。

－注意喚起ページからは他にも長期休暇に関係なく常時から注意すべき普遍的なものをまとめた「日常的に実施すべき情報セキュリティ対策」にもリンクしており、それぞれにおいて準備・点検を行うよう意識していくことが肝要です。