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。

●パスワードマネージャーに対する「クリックジャッキング」攻撃、カード情報等が自動入力で流出の恐れ

https://pc.watch.impress.co.jp/docs/news/2040344.html
https://socket.dev/blog/password-manager-clickjacking

このニュースをザックリ言うと・・・

- 8月20日(現地時間)、米Socket社より、パスワードマネージャーに保存された機密情報を奪取する攻撃について注意喚起が出されています。

- 手法は8月上旬に米国で開催されたハッキングカンファレンス「DEF CON 33」でセキュリティ研究者によって発表されたもので、拡張機能の設定でパスワード等の自動入力が有効となっている場合、いわゆる「クリックジャッキング」攻撃と組み合わせることにより、攻撃者が仕掛けた不審なフォームに情報を自動入力させ、これを読み取ったり、外部に送信させたりするシナリオが可能になるとされています。

- セキュリティ研究者のページではデモページが用意されており、また1Password・Bitwarden・iCloud Passwords・LastPass等多くのパスワードマネージャーで攻撃が有効とされています(Dashlane・Enpass・Keeper・NordPass・ProtonPass・RoboFormでは対策済みとされています)。

AUS便りからの所感等

- 注意喚起等においては、Webサイトへのアクセス時にCookieを受け入れるか否か選択するボタンの裏に、情報を自動入力させるための入力欄を透明化した状態で配置する等の例が挙げられています。

- パスワードマネージャーに保存されている情報のうち、Webサイトへログインするためのアカウント情報についてはドメイン名が正しくない場合に自動入力されないものの、クレジットカード情報や氏名等の個人情報については、そのような制限がなく、フィッシングサイト等であっても自動入力される可能性があります。

- また広義のクリックジャッキングと異なり、外部にある本物のWebサイトのコンテンツをインラインフレームで埋め込む必要もないとみられます。

- 前述したもの含め、各種パスワードマネージャーにおける問題の有無、対策状況はまちまちであり、使用しているもので対策されたとしても、自動入力設定は無効にすることを強く推奨致します。

Impress Watch

Cookieを許可したらアカウント情報が流出!? パスワード自動入力を悪用した攻撃に注意

宇都宮 充　2025年8月20日 17:25

セキュリティ企業のSocketは8月20日、パスワードマネージャーが持つアカウント情報などの自動入力機能を悪用した攻撃について紹介。自動入力の表示の上に、別の要素を重ねて表示することで、ユーザーが意図せずプライベート情報を入力してしまうように仕向ける「クリックジャッキング攻撃」が可能だとし、注意を呼びかけている。

この手法は、世界最大級のハッキング/セキュリティカンファレンスであるDEF CON 33にて、セキュリティ研究者のMarek Tóth氏が報告したもの。パスワードマネージャーには、IDやパスワード、クレジットカード番号などの自動入力機能を持つものがあるが、これを悪用して機密情報の窃取を狙うという。

● AppleよりiOS・iPadOS・macOSセキュリティアップデート、重大な脆弱性に対応

https://www.itmedia.co.jp/mobile/articles/2508/21/news112.html
https://support.apple.com/en-us/124925

このニュースをザックリ言うと・・・

- 8月20日(現地時間)、Apple社より、iOSの最新バージョン18.6.2がリリースされました。
- 悪意のある画像の表示によって攻撃可能とされる脆弱性1件(CVE-2025-43300)の修正ですが、「特定個人をターゲットとした非常に高度な攻撃に悪用された可能性がある」とされています。
- 同社からはこの他にもiPadOS 18.6.2・17.7.10、macOS Sequoia 15.6.1・Sonoma 14.7.8・Ventura 13.7.8も同時にリリースされ、いずれも「重要なセキュリティ修正が含まれ、すべてのユーザーに推奨」とされています。

AUS便りからの所感

- 脆弱性はメモリ破壊を引き起こすもので、機器の強制再起動以外にも任意のコードの実行等にも繋がるとみられます。
- Android等と同様、OSのアップデートは定期あるいは不定期に行われるものですが、こと今回のように不正な画像を含むWebサイトやメールの閲覧で攻撃され得るような脆弱性を修正するものものについては、速やかにアップデートの適用を行うよう計画すべきでしょう。

●7月度フィッシング報告件数は226,433件、証券会社騙るフィッシング再び増加

https://www.antiphishing.jp/report/monthly/202507.html

このニュースをザックリ言うと・・・

- 8月21日(日本時間)、フィッシング対策協議会より、7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。
- 7月度の報告件数は226,433件で、6月度(https://www.antiphishing.jp/report/monthly/202506.html)の192,870件から33,563件増加しています。
- 悪用されたブランド件数は97件で6月度(94件)から3件増加、割合が多かったものとしてSBI証券(16.1%)、NTTドコモ(13.2%)、Apple(約7.0%)、ANA(約6.9%)が挙げられ、次いで1万件以上報告されたVISA、松井証券と合わせて約58.3%、さらに1,000件以上報告された35ブランドまで含めると約94.4%を占めたとのことです。
- フィッシングサイトのURL件数は85,272件で6月度(60,107件)から25,165件増加、使用されるTLD(トップレベルドメイン名)の割合は10,000件以上の報告があった .cn(約26.4%)、 .top(約22.4%)、 .com(約21.9%)および.cc(約4.7%)で約75.3%を占めています。

AUS便りからの所感

- 同協議会では7月度の報告件数について、証券会社からの多要素認証設定依頼や補償に関するメール等を装ったフィッシングメールの配信が再び増加したためとしています。
- フィッシングサイトのTLDは、.cnが4・5月度の落ち込みを経て6月度以降再び最も割合が多くなっており、この他では.topが先月度の約8.8%から急増しています。
- また今回、アカウントの乗っ取りや不正契約等による、国内ホスティングサービス・ISPのIPアドレスからのフィッシングメールの発信も増えているとしており、特に正規のメールアカウントの乗っ取りでなりすましメールを送信されることは、組織に対する信頼の毀損に関わる恐れがありますので、PC側のアンチウイルス・UTMによる保護とともに、サーバー側においてもメールアカウントへの不正ログイン試行を監視・検知・遮断する体制を整えることが重要です。

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