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。

●7月度フィッシング報告件数は66,119件…使用されるクラウドサービスも流動か

https://www.antiphishing.jp/report/monthly/202607.html

このニュースをザックリ言うと・・・

－8月17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66,119件で、6月度(https://www.antiphishing.jp/report/monthly/202606.html)の72,370件から6,251件減少しています。

－悪用されたブランド件数は101件で6月度(98件)から3件増加、最も報告が多かったブランドはAmazonが約37.0%、次いでApple(約11.8%)、セゾンカード(約7.7%)、JCB、イープラスと合わせて約68.6%、さらに1,000件以上報告された11ブランドまで含めると約84.4%となっています。

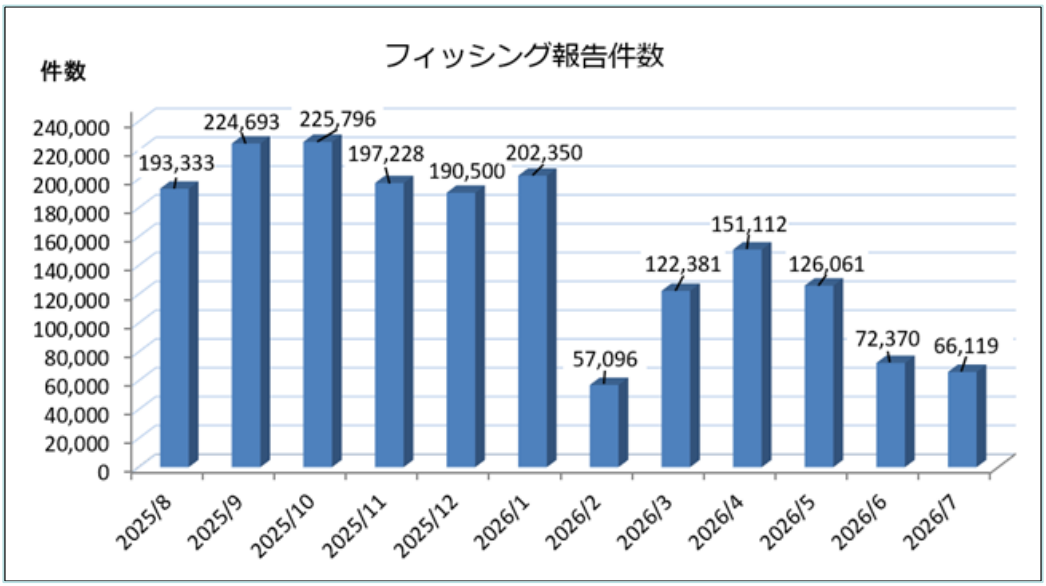
AUS便りからの所感等

－毎月のフィッシング報告件数については、2025年3月に現在まで最多となる249,936件を記録し、以後2026年1月まで19万件超を維持していましたが、1月末に海外におけるレジデンシャルプロキシおよびボットネットの無力化が行われてからは、4月の151,222件を一時的な増加のピークとして低い水準が続いており、また日平均の報告件数も7月は6月に比べ279件減少しているとのことです。

－フィッシングメールの発信元は既に中国からの割合は低く、今やアメリカでホスティングされているクラウドサービスが大多数とされ(この他シンガポール発も増加)、これに伴いPTRレコード(IPアドレスからの逆引き)設定のないIPアドレスからの発信も約39.4%と減少している一方、そのクラウドサービスの割合もGoogle Cloudが約86.7%→約10.7%、Microsoft Azureが約8.0%→約52.5%と変動(この他BytePlus 約24.3%)しています。

－7月度は実在のドメイン名になりすましたフィッシングメールが約26.5%と比較的多く、うちDMARC(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)ポリシーがreject(受信拒否)ないしquarantine(迷惑メールフォルダー等への隔離)に設定されているドメイン名だったものが約13.7%、none(検証可否に拘らず素通し)が約6.7%、DMARC未設定が約6.1%とされ、半数近くが検知が期待できるケースでも構わずになりすましを行っていた傾向がみられますが、ともあれ自組織ドメイン名のDMARCポリシーは最低でもquarantineとし、「事業者のみなさまへ」でも呼び掛けられている通り、最終的にrejectに変更するまでの計画を立てることにより、取引相手等をなりすましから確実に守るよう動いて頂ければ幸いです。

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



● 8月の「パッチチューズデー」MS等セキュリティアップデート…夏季休暇明けにも必ず適用を

https://forest.watch.impress.co.jp/docs/news/2132160.html
https://www.microsoft.com/en-us/msrc/blog/2026/08/202608-security-update
https://forest.watch.impress.co.jp/docs/news/2132308.html
https://forest.watch.impress.co.jp/docs/news/2132325.html

このニュースをザックリ言うと･･･

- 8月12日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 11 24H2・25H2 KB5121003(ビルド 26100.9168・26200.9168)および11 26H1(一部機種で使用) KB5121000(ビルド 28000.2704)等となります。
- 修正された脆弱点は421件とされ、7月の622件に次ぐ規模となっています。
- この日はChromeブラウザーも5件の脆弱点を修正した151.0.7922.138(Windows)がリリース、Adobe社からはColdFusion等5製品についてセキュリティ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

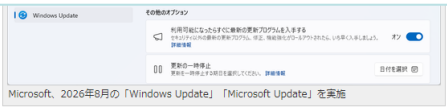
- 修正された脆弱点のうち62件において危険度が4段階中最高の「Critical」とされ、またそれ以外でも3件がパッチ公開前の時点で悪用を確認ないし詳細が公開済みとされています。
- またFirefoxブラウザーも153.0.4がリリース(不具合修正が発表されていますがセキュリティアップデートかは不明です)、またEdgeブラウザーは11日に151.0.4129.78がリリースされています。
- Windows 11 24H2は10月14日でサポート終了予定とされており、25H2以降へのアップグレードが強く推奨されています。
- 今回の「パッチチューズデー」は夏季休暇の時期と重なり、ある程度のタイムラグが発生した企業・組織も多々あるとみられますが、速やかにアップデートを実施すること、以後も各種ソフトウェアの定期的なパッチリリースに対し計画的なアップデートと、アンチウイルス・UTM等による多重防御を適切に行うことを常に心掛けましょう。

Impress Watch

Microsoft、2026年8月の「Windows Update」 ～脆弱性修正は421件で非常に大規模、悪用確認済みも1件

「緊急」は62件。先月からは大きく減ったが、依然として大規模なセキュリティパッチに

樽井 秀人　2026年8月12日 08:02



Microsoft、2026年8月の「Windows Update」「Microsoft Update」を実施

米Microsoftは8月11日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Microsoft Update カタログ」などから入手可能。

リリースノートによると、今月修正されたCVEは421件。過去最多を記録した先月の622件からは大きく減ったものの、歴史的に見れば依然として巨大な規模だ。

●WordPressに「XSS2Shell」等脆弱点報告相次ぐ、7.0.4への更新確認を

https://wordpress.org/news/2026/08/wordpress-7-0-3-release/
https://wordpress.org/news/2026/08/wordpress-7-0-4-release/
https://finance.biggo.jp/news/cc9d5925-9ec8-4c74-8e10-d87b113d17fc

このニュースをザックリ言うと･･･

- 8月前半において、WordPressのセキュリティアップデートが2度にわたってリリースされています。
- 8月7日(日本時間)リリースの7.0.3では12件の脆弱点が修正され、特にログイン画面に存在する脆弱点「CVE-2026-64638」については、これを報告したセキュリティ企業pwn.aiにより「XSS2Shell」と名付けられ、危険度が高いものとして注意喚起が出されています。
- 次いで同13日にも7.0.4がリリースされ、同じくpwn.aiが報告した、不正なメディアファイルのアップロードにより攻撃可能とされる脆弱点「CVE-2026-65640」1件が修正されています。
- 7月18日に7.0.2等で修正された脆弱点「wp2shell」は6.9・7.0系に影響するものでしたが、今回は6.8系以前のさらに古いバージョンにも影響するとされ、7.0.4・6.9.7の他、4.7～6.8系においても修正バージョン(6.8.8・6.7.7等)がリリースされています。

AUS便りからの所感

- XSS2Shellはログイン失敗時のエラー画面に存在する脆弱点とされ、クロスサイトスクリプティング(XSS)から、サーバー上でのPHPコードの実行にまで至るものとされています。
- CVE-2026-65640の悪用には、攻撃者が何らかのファイルをアップロード可能であることが条件とされ、通常は「投稿者(Author)」以上の権限を持つユーザーとしてログインする必要がありますが、サイト上にフォームを設置し、ファイルのアップロードも受け付けている場合、ログインしていなくても攻撃が可能となる恐れがあるとされていることには注意が必要です(また当該脆弱点はImagickモジュールおよびGhostscriptの導入も条件となりますが、サイトによって有効かどうか、また無効に設定できるかはまちまちとみられます)。
- 様々なソフトウェアにおいてAIによる脆弱点報告が急増し、WordPress本体においても7.0.2～7.0.4とこれまでにない頻度でアップデートが行われる事態となっており、(プラグイン等も含め)毎回のアップデートを速やかに適用できる体制を整え、セキュリティ系プラグインをインストールし、WAFの導入についても検討する等、多重防御を心掛けるべきでしょう。

2026年8月13日
sysbird による

WordPress 7.0.4リリース

WordPress 7.0.4を利用できます。

WordPress 7.0.4がリリースされました。このバージョンでは、セキュリティ修正が行われています。セキュリティリリースであるため、お使いのサイトを直ちに更新することをお勧めします。

WordPress 7.0.4への更新は、WordPress.org からダウンロードするか、サイトのダッシュボード→「更新」にアクセスして「今すぐ更新」をクリックすることで行えます。自動バックグラウンド更新に対応しているサイトでは、まもなく更新が開始されます。

詳細については、WordPress 7.0.4 HelpHub サイトをご覧ください。

このリリースに含まれるセキュリティ更新

セキュリティチームは、脆弱性を責任ある形で報告していただき本リリースでの修正につながった pwn.ai チームに感謝します:

- Imagick と Ghostscript を使用するサイトで、認証済みの投稿者以上の権限を持つユーザーが悪意のあるファイルをアップロードすることによって発生するリモートコード実行の脆弱性。