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。

●9月の「パッチチューズデー」…MSセキュリティアップデートは過去最大規模

https://forest.watch.impress.co.jp/docs/news/2139296.html
https://www.microsoft.com/en-us/msrc/blog/2026/09/202609-security-update
https://forest.watch.impress.co.jp/docs/news/2139344.html

このニュースをザックリ言うと・・・

- 9月9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 KB5124008(ビルド 26100.9445・26200.9445)および11 26H1(一部機種で使用) KB5124012(ビルド 28000.2704)等となります。
- 修正された脆弱点はCVEベースで974件とされ、7月の622件を凌ぐ過去最大規模となっています。
- うち114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2件がパッチ公開前の時点で悪用を確認したとされています。

AUS便りからの所感等

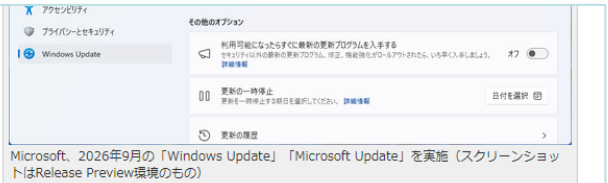
- 危険度「Critical」の一例として、WindowsのDNSサーバーにおける任意のコード実行の脆弱点「CVE-2026-69730」が挙げられており、Windows Server等でDNSサーバーが起動している場合、細工したパケットを送信することにより、サーバーを乗っ取られる恐れがあるとされています。
- 2020年7月に同じくWindowsのDNSサーバーで修正された脆弱点「SIGRed(CVE-2020-1350)」はワームの拡散に悪用される恐れも指摘されていましたが、今回の脆弱点はその後継として同様にターゲットとされる可能性がある模様で、ActiveDirectoryのドメイン構築のため当該DNSサーバーを導入している企業等においては特に速やかなパッチの適用等が必要となるでしょう。
- いわゆる「パッチチューズデー」にあたるこの日はAdobe社からもAcrobat/Reader 26.002.21901やPhotoshop・Illustrator等9製品へのセキュリティアップデートがリリースされる等、各社のアップデートが集中しており、このような定期的アップデートのスケジュールについて、特にシステム管理者においては忘れず意識し、OS・機器のファームウェアから各種アプリケーションに至るまで脆弱性への根本的対策としてのアップデートの適用を必須とし、加えてアンチウイルス・UTM等による多重防御策により、適用前の脆弱性への攻撃に備えるようにしてください。

Impress Watch

脆弱性974件、過去最多を大幅に更新 ～Microsoftが2026年9月「Windows Update」を実施

「緊急」は114件。悪用確認済みは2件。タスクバー、スタート、検索の刷新も一般展開へ

樽井 秀人　2026年9月9日 08:50



Microsoft、2026年9月の「Windows Update」「Microsoft Update」を実施（スクリーンショットはRelease Preview環境のもの）

米Microsoftは9月8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974件。先月の421件から倍増しただけでなく、これまで最多だった7月の622件も大幅に上回り、記録を更新した。

●不審なアプリインストールから不正送金に…PayPayが注意喚起

https://www.itmedia.co.jp/news/article/2609/09/2000001306/
https://paypay.ne.jp/notice/20260907/s-01/

このニュースをザックリ言うと・・・

- 9月7日(日本時間)、PayPayを運営するPayPay社より、スマートフォンがマルウェアに感染、遠隔操作による不正な送金等の事例が確認されているとして注意喚起が出されています。

- 不審なメールやSNS上の広告等から誘導されたサイト・リンク先からアプリをダウンロード・インストールすることで発生するとされています。

- 同社ではこのような形で誘導されたサイト・リンク先からアプリをダウンロード・インストールしないこと、PayPayアプリの「取引履歴」から、身に覚えのない送金や決済がないか確認することを呼び掛けています。

AUS便りからの所感

- 不正なアプリのダウンロード経路の例として、当初注意喚起では「公式アプリストア(App Store、Google Play)以外のサイト」が挙げられていました。

- 2025年施行のいわゆる「スマホ新法」により、上記以外のアプリストア参入等の競争が促進されている一方で、安全でない経路でのアプリインストールについて障壁が下がること等によるセキュリティリスク上昇の懸念が当初から指摘されています。

- 現在でも公式アプリストア以外からのアプリのインストールには設定変更が必要とされ、安易にその制限を解除するようなことはせず、周辺の評価を確認する等、十分な考慮を行うこと、また複数の端末を持っている場合、決済・送金といった重要な役割を持つ端末に関しては公式サイトから必要最低限のアプリをインストールのみに留める等管理すること、そしてどの端末においてもOSないし各アプリを最新バージョンに保つことが肝要です。

●数百のWordPressサイトで改ざん被害…訪問者にClickFix攻撃、認証情報を奪取

https://cyber.nexsight.co/articles/2026/09/02/netskope-amatera-etherhiding-service-worker-2026-09-02/
https://www.netskope.com/blog/etherhiding-in-the-browser-clickfix-chain-ends-in-amatera
https://patchon.jp/blog/fake-recaptcha-service-worker

このニュースをザックリ言うと・・・

- 8月27日(現地時間)、セキュリティベンダーのNetskope社より、数百のWordPressが改ざんの被害を受け、「ClickFix」攻撃を行う仕掛けが仕込まれるケースが確認されたとして注意喚起が出されています。

- 攻撃により、WordPressに不正な「must-useプラグイン(mu-plugins)」が導入、サイト訪問者のブラウザー上で「Service Worker」を起動し、偽のCAPTCHA画像やClickFixを行うプログラムを外部のブロックチェーン上から読み込んで実行させるとしています。

- ClickFixにより、「Amatera」と呼ばれるインフォスティーラーが実行され、ブラウザー上から認証情報が奪取されるとしています。

AUS便りからの所感

- must-useプラグインはWordPressの正式な機能(https://ja.wordpress.org/support/article/must-use-plugins/)で、サイト上で自動的に読み込まれ、無効化できない特別なプラグインをwp-content/mu-plugins/ディレクトリ下にインストールするものであり、攻撃者は不正なプラグインの本体として「site-helper-」で始まる名前のファイルを配置することにより、この機能を悪用するとしています。

- 不正なプラグインはサイトのログインユーザーに対しては動作せず、外部の訪問者に対してのみ動作し、管理者から認知されにくい挙動を示す模様です。

- 注意喚起では、前述したmust-useプラグインファイルの他、Webサイト上に身に覚えのないfront-probe.js・nochain-sw.js・nc-dropin.php等のファイルがあれば削除すること等を呼び掛けています。