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。

●1月の「パッチチューズデー」、Microsoft・Adobe等月例セキュリティアップデート

https://forest.watch.impress.co.jp/docs/news/2077586.html
https://msrc.microsoft.com/blog/2026/01/202601-security-update/
https://forest.watch.impress.co.jp/docs/news/2077632.html
https://forest.watch.impress.co.jp/docs/news/2077665.html

このニュースをザックリ言うと・・・

- 1月14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 KB5074109(ビルド 26100.7623・26200.7623)および11 23H2 KB5073455(ビルド 22631.6491)となります。

- この日はMSを中心とした各社のアップデート集中日、いわゆる「パッチチューズデー(米国時間での第2火曜日にあたる)」で、同日にはAdobe社よりDreamweaver・InDesign・Illustrator・ColuFusion等11製品についてセキュリティアップデートが、またGoogle社からもChromeブラウザーのメジャーアップデートとなる144.0.7559.59/60(Windows版)がリリースされています。

AUS便りからの所感等

- MS製品で修正された脆弱点のうちWindowsの4件が既に悪用が確認ないし攻撃手法が公開済みとされ、またWindows・Officeの8件について危険度が4段階中最高の「Critical」と評価されています。

- Adobe製品の脆弱点においてもColdFusionの1件について、危険度が3段階中最高とされています。

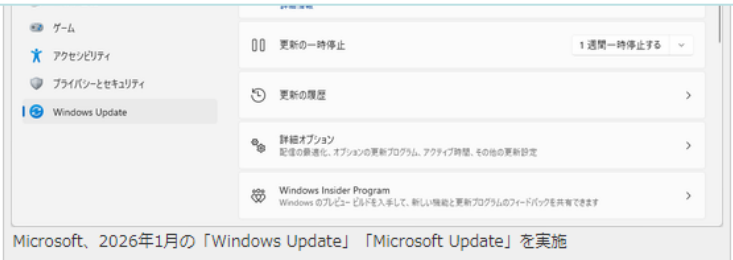
- ColdFusionの基盤にもなっているJavaを含めたOracle社製品については、翌週1月21日に四半期毎のアップデートリリースが予定されており、システム管理者においてはこのようなソフトウェアベンダー各社による定期的なアップデートスケジュールを把握し、OS・ファームウェアないし各種アプリケーションを最新に保つこと、併せてアンチウイルス・UTM等による多重防御を適切に行うことを常に心掛けてください。

Impress Watch

Microsoft、2026年最初の「Windows Update」を実施 ～ OS、Word、Excelなどに致命的な脆弱性

悪用が確認された脆弱性も、すぐに更新を

樽井 秀人　2026年1月14日 09:58



Microsoft、2026年1月の「Windows Update」「Microsoft Update」を実施

米Microsoftは1月13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「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで112件（サードパーティーも含めると114件）の脆弱性が新たに対処されている。

● Instagramユーザー1,750万人分の個人情報流出か、パスワードリセット試行の報告相次ぐ

https://gigazine.net/news/20260111-instagram-big-data-breach/
https://www.malwarebytes.com/blog/news/2026/01/received-an-instagram-password-reset-email-heres-what-you-need-to-know
https://gigazine.net/news/20260113-instagram-password-reset-email/

このニュースをザックリ言うと・・・

- 1月11日(米国時間)、セキュリティベンダーのMalwarebytes社より、Instagramのユーザーがパスワードリセットのリクエストに関するメールを受け取ったとする報告が相次いだとして注意喚起が出されています。

- 同社によれば、これと並行して、Instagramユーザー1,700万人分(IT系メディアでは1,750万人分とされています)の個人情報(ユーザー名・氏名・ID・メールアドレス・電話番号および位置情報)がダークウェブで販売されていることを確認したとしています。

- Instagram側は今回侵害を受けたことは否定しており、X(旧・Twitter)にて、外部からパスワードリセットのリクエストが可能になる問題を修正したとし、今回届いたメールは無視するよう呼び掛けています。

AUS便りからの所感

- Instagramでは2019年等にもユーザー情報が流出した事案があり(AUS便り 2019/5/27号参照)、今回ダークウェブで販売されていたとするデータはこのような過去に流出したデータである可能性もMalwarebytes社等から指摘されています。

- 攻撃者が奪取したユーザー情報(特にメールアドレスと電話番号)はパスワードリセットのリクエスト以外にもアカウント奪取を狙ったフィッシング等のターゲットとされる恐れがあり、セキュリティ技術者により、アカウントを保護するためのいくつかの手順をとることが推奨されており、例えばパスワードリセットのメールがInstagramから送られた本物のメールであるか、アカウントセンターの「パスワードとセキュリティ」(https://help.instagram.com/760602221058803)から確認すること等を挙げています。

- InstagramではGoogle Authenticator等の認証アプリもしくはSMSでコードを入手する2要素認証(2FA)を提供していますが、電話番号も流出している可能性があることもあり、SMSによる2FAは十分に安全でなく、認証アプリを用いることが推奨されている模様です。

●node.jsセキュリティアップデートリリース…12月予定から延期を経て

https://forest.watch.impress.co.jp/docs/news/2077577.html
https://nodejs.org/en/blog/vulnerability/december-2025-security-releases

このニュースをザックリ言うと・・・

- 1月13日(米国時間)、JavaScript実行環境「Node.js」のセキュリティアップデート(25.3.0, 24.13.0, 22.22.0, 20.20.0)がリリースされています。

- 8件の脆弱性を修正するものとなっており、悪用により、Webサーバー上の機密情報やファイルへの不正な読み書き、およびDoS攻撃等が行われる恐れがあるとされます。

- 当初12月15日リリース予定とのことでしたが、延期となっていたものです。

AUS便りからの所感

- 現在node.jsのアップデートは最新メジャーバージョン25系およびLTS(長期サポート)対象の24・22・20系についてのみリリースされており、これ以外の系列は既にサポートが終了しているため、依然使用している場合はメジャーバージョンの変更を強く推奨致します。

- Webアプリケーションに対する外部からの不正なリクエストの送信により、脆弱性を悪用される可能性があるため、根本的対策のためセキュリティアップデートを適用するのと併せて、可能であればWAFの導入も検討すべきでしょう。

- この他、npm等によってインストールされたnode.js用ライブラリに悪意のあるコードが含まれている場合、内側から脆弱性の悪用をはじめとした攻撃を行われる可能性も考えられるため、ライブラリを導入する側がSNS等で最新バージョンに関する問題の報告がないか確認しつつ、安全なバージョンをインストールするよう注意を払うことも重要です。