

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。

●Microsoft・Adobe・Apple等、月例のセキュリティアップデートリリース

<https://forest.watch.impress.co.jp/docs/news/1669503.html>
<https://msrc.microsoft.com/blog/2025/03/202503-security-update/>
<https://forest.watch.impress.co.jp/docs/news/1669505.html>
<https://forest.watch.impress.co.jp/docs/news/1669506.html>
<https://forest.watch.impress.co.jp/docs/news/1669502.html>



このニュースをザックリ言うと…

- 3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 10 22H2 KB5053606(ビルド 19045.5487)、11 23H2 KB5053602(ビルド 22631.5039) および 11 24H2 KB5053598(ビルド 26100.3476) 等となります。
- 同日にはAdobe社より「Acrobat」「Acrobat Reader」「Illustrator」等6製品について、Apple社からも「Safari」「iOS」「iPadOS」「macOS」等について脆弱性が報告され、セキュリティアップデートがリリースされています。

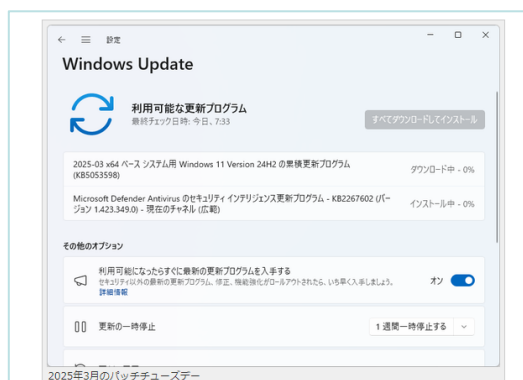
AUS便りからの所感等

- MSの月例アップデートでは7件の脆弱性が既に悪用ないし攻撃コードが出回っているを確認、Office・DNSサービス・リモートデスクトップ(クライアント・サービスとも)等6件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。
- Appleのセキュリティアップデートは各製品に共通して使用されるWebKitの脆弱性「CVE-2025-24201」の修正がメインとなっており、これも既に悪用が確認済みとされています。
- またGoogle Chromeも3月11日にv134.0.6998.88/89がリリースされていますが、Mac版においては前述のCVE-2025-24201の影響を受けるとされ、同様に修正されています。
- 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)」におけるMS他の月例のセキュリティアップデートをはじめ、各種ソフトウェアベンダーが定期的(隔月・四半期毎等)に行うアップデートについて、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計画的に更新、加えてアンチウイルス・UTM等による多重防御策により、常に脆弱性への攻撃に備えるよう心掛けてください。



2025年3月の「Windows Update」が公開 〜ゼロデイ脆弱性、致命的な脆弱性多数
CVE番号ベースで56件に対処

橋井 秀人 2025年3月12日 08:42



米Microsoftは3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「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56件(サードパーティーのものも含めれば67件)の脆弱性が新たにに対処されている。

●コードエディター「Visual Studio Code」拡張機能に不審なコードか… 公式ストアから削除



<https://news.mynavi.jp/techplus/article/20250228-3137463/>

<https://medium.com/extensiontotal/a-wolf-in-dark-mode-the-malicious-vs-code-theme-that-fooled-millions-85ed92b4bd26>

このニュースをザックリ言うと…

- 2月26日(現地時間)、インターネットメディア「Medium」にて、Microsoft(以下・MS)製コードエディター「**Visual Studio Code(VSCode)**」の**拡張機能に不審なコード**を含むものが確認されたと報じられています。
- 問題となったのはVS Codeの見た目をカスタマイズする「**Material Theme - Free**」「**Material Theme Icons - Free**」で、いずれも**MS公式の拡張機能マーケットプレイスに登録**されていたものです。
- 指摘を受けてMSではマーケットプレイスから当該拡張機能を削除していますが、これらは**削除される前に併せて900回以上ダウンロード**されていたとのこと。

AUS便りからの所感

- VSCodeは開発者から人気の高いコードエディターの一つで、ソースコードのハイライトや、GitHub等または内部のソースコード管理サーバーへのアクセスを容易にする等の目的で**多数の拡張機能が開発・提供**されています。

- VSCodeで拡張機能から実行できる機能の範囲は**Chrome・Firefox等のWebブラウザのそれと同様**であり、VSCodeにインストールされる拡張機能はVSCode上で**様々な機能の使用を許可されることになり、悪意のある拡張によってはPC上の任意のファイルを読み取られ、機密情報を奪取される恐れ**もあります。

- ブラウザーの拡張あるいは**スマートフォンアプリと同様、マーケットプレイス上やSNS上でのレビュー等を十分に確認し、必要最低限の拡張機能のみインストール・有効化すること、身に覚えのない拡張機能が入っていれば速やかにアンインストール**することが重要です。



VS Codeの人気拡張機能にマルウェア、すぐに削除を - 900万回以上DL

掲載日 2025/02/28 12:17

寄稿：後藤大地

Mediumは2月26日(米国時間)、「A Wolf in Dark Mode: The Malicious VS Code Theme That Fooled Millions」by Amit Assaraf | ExtensionTotal | Feb, 2025 | Medium」において、Microsoft Visual Studio Codeの人気拡張機能からマルウェアを発見したと報じた。

マルウェアは2つの拡張機能から発見され、これらの合計ダウンロード数は900万回以上と見られる。これら拡張機能は報告後、Microsoftにより削除された。

● JavaScript実行環境「Node.js」サポート切れバージョンそのものに CVE申請も却下される



<https://forest.watch.impress.co.jp/docs/news/1668795.html>

<https://nodejs.org/en/blog/vulnerability/updates-cve-for-end-of-life>

このニュースをザックリ言うと…

- 3月7日(現地時間)、JavaScript実行環境「**Node.js**」開発元より、Node.jsの**サポートが切れた古いバージョンの存在そのものを脆弱性とするCVE番号の割り当てが却下**されたと発表されました。

- 開発元では1月に、サポート切れとなっている**バージョン17系以前・19系・21系**の使用をそれぞれ「CVE-2025-23087」「CVE-2025-23088」「CVE-2025-23089」として採番していましたが、今回CVEを管理するMITREより、**特定の脆弱性に対してCVE番号を割り当てるという現行のルールに即しない**として却下されたとしています。

- Node.jsでは現時点で**最新バージョンの23**の他、**LTS(長期サポート)**対象となっている**バージョン18・20・22系でセキュリティサポート**を行っており、これらで**確認された脆弱性は今後サポート切れバージョン全てで影響するものとして扱う**としています。

AUS便りからの所感

- 開発元によれば、やはり**サポート切れ済みのバージョン16**が**現在も月間1,100万以上ダウンロード**されているとのこと(古いLinuxディストリビューションで18以降が使用できない場合があるためと推測されます)。

- Node.jsの他、Javaや.NET(5以降)等においては、**メジャーバージョン毎に特定のルールでLTS指定が行われ、バージョン毎にサポート期間が異なるため、常に現行での最新バージョンを採用することが長期のサポートを得られるわけではない**ことに注意し、**適切に使用するバージョンの選定**を行うべき場面があるでしょう。

- ともあれ、**どのソフトウェアでもサポートされていない古いバージョンを使い続けることは脆弱性のリスクがあることに留意し、計画的にアップデートを行うよう意識**することが肝要です。



EOLを迎えた古い「Node.js」へのCVE付番、MITREに却下されてしまう

開発チームが新方針発表、EOL版は便宜上「今後の新たな脆弱性全てが該当する」原則に

橋井 秀人 2025年3月10日 12:38

ライフサイクルを終えた(EOL)古い「Node.js」バージョンに付番したCVE番号は、MITREによって却下されてしまったとのこと。「Node.js」の開発チームが3月7日、公式ブログで明らかにした。

「Node.js」の開発チームは2025年1月のセキュリティアップデートを機に、セキュリティパッチの提供を終了した古いバージョンを利用することを脆弱性とみなし、以下のCVE番号を付与した。

- **CVE-2025-23087**：「Node.js」v17およびそれより前のすべてのバージョンの利用
- **CVE-2025-23088**：「Node.js」v19の利用
- **CVE-2025-23089**：「Node.js」v21の利用

これはEOLバージョンの実行がセキュリティ上望ましくないことを強調し、アップグレードを推奨することを意図したものだったが、CVE番号は本来、特定の脆弱性のみが付番されるべきものだ。そのため、協議の結果、サポート終了製品への付番は却下されてしまった。将来的に認められる可能性はあるものの、現時点では原則に外れる運用だと判断されたようだ。