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。

●ClickFixのさらなる亜種、不正なChrome拡張機能から攻撃する「CrashFix」

https://forest.watch.impress.co.jp/docs/news/2084493.html
https://www.microsoft.com/en-us/security/blog/2026/02/05/clickfix-variant-crashfix-deploying-python-rat-trojan/
https://www.huntress.com/blog/malicious-browser-extention-crashfix-kongtuke

このニュースをザックリ言うと・・・

- 2月5日(米国時間)、Microsoftより、いわゆる「ClickFix」攻撃の新たな亜種「CrashFix」について注意喚起が出されています。

- CrashFixは意図的にブラウザーをクラッシュさせるよう誘導し、解決策と偽ってバックドアが仕込まれるような悪意のあるスクリプトを、ClickFixと同様に「Win+R」「Ctrl+V」「Enter」という手順で実行させようとします。

- 攻撃はGoogle公式のChromeブラウザー拡張機能ストアに登録された「NexShield」という偽の広告ブロック拡張機能から実行されていたとのことです(現在は削除されています)。

AUS便りからの所感等

- ClickFixの亜種は1月にも偽のブルースクリーン(BSoD)を表示してスクリプトを実行させる「PHALT#BLYX」が報告されており(AUS便り 2026/01/09号参照)、今回のCrashFixについても1月16日の時点でセキュリティ企業のHuntress社に取り上げられていたもので、Microsoftの記事もこれを参考にしています。

- 前述のPHALT#BLYX同様に「サポート詐欺」の如く相手を混乱させ、正常な判断をさせずにそこからClickFixと同様の手口に追い込むものであり、主な攻撃の経路はサポート詐欺が悪意のある広告、ClickFixがフィッシングサイト、今回のCrashFixが悪意のある拡張機能と様々です。

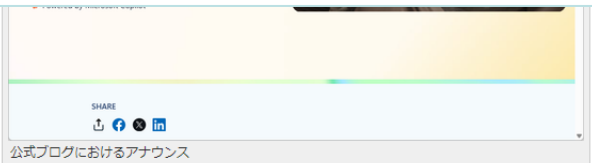
- また悪意のある拡張機能についても公式ストアに多数アップロードされていた事例が12月に報告されています(同2025/12/05号参照)が、Webブラウザーにインストールした拡張機能は様々な機能の使用を許可されることに十分注意し、ネット上での報告等も参考にしつつ、検索で出てきた拡張機能を安易にインストールしないよう心掛けましょう。

Impress Watch

バックドアを仕掛けられるおそれ ～Microsoft、「ClickFix」の亜種「CrashFix」を警告

自らトラブルを引き起こしておいて『助ける』と騙すマッチポンプな攻撃が特徴

樽井 秀人　2026年2月9日 13:06



公式ブログにおけるアナウンス

米Microsoftは2月5日（現地時間）、「ClickFix」の新しい亜種「CrashFix」を確認したと発表した。2026年1月に発見されたとのことで、公式ブログでその詳細が明らかにされている。

「ClickFix」は、Webページの閲覧中に『PCのトラブルを解決する』などとユーザーを騙し、ボタンをクリックして悪意あるコードを実行させるタイプの攻撃手法。『サブスクが無料になる裏ワザがある』と偽り、［ファイル名を指定して実行］ダイアログ（［Windows］＋［R］キー）から悪意あるコマンドを実行させたりするケースもあり、最近は多様化・巧妙化しつつある。少し前に紹介した、［ファイル名を指定して実行］ダイアログを使わない「FileFix」も「ClickFix」の派生版だ。

● Chromeに緊急セキュリティアップデート、v145.0.7632.75/76への更新確認を

https://forest.watch.impress.co.jp/docs/news/2085987.html
https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
https://forest.watch.impress.co.jp/docs/news/2085297.html

このニュースをザックリ言うと・・・

- 2月14日(日本時間)、Google社より、Chromeブラウザーのセキュリティアップデートとして最新バージョン145.0.7632.75/76がリリースされています。

- 同11日にメジャーアップデートとなる145.0.7632.45/46がリリースされるとともに11件の脆弱点が修正されていましたが、CSSに関するゼロデイの脆弱点(CVE-2026-2441)が報告され、緊急に修正が行われたとしています。

AUS便りからの所感

- Chromeを長期間アップデートしていない場合、右上に「更新して再起動」のボタンが表示されますが、ボタンをクリックして一度更新を適用しても145.0.7632.45/46あるいは同13日リリースの145.0.7632.68に留まっている可能性があり、再起動後も改めて「ヘルプ」→「Google Chromeについて」(あるいはchrome://settings/help)にアクセスすることにより、バージョン情報を確認するとともに、アップデートが残っている場合に適用する必要があります。

- Chromeブラウザーは概ね日本時間の毎週水曜日にアップデートがリリースされており、この日の朝～昼頃に上記の手順でアップデートを確認することをまずルーチンとすべきですが、今回のように水曜のリリース後2度にわたってさらなるリリースが発生するケースもあり、万全を期すならばより高い頻度、例えば一日に一度確認する等で、確実に最新バージョンに保つよう努めるとなお良いでしょう。

Impress Watch

リリースされたばかりの「Google Chrome 145」にゼロデイ脆弱性、修正版が緊急公開

Windows環境ではv145.0.7632.75/76が展開中

樽井 秀人　2026年2月16日 00:05

米Googleは2月13日（現地時間）、デスクトップ向け「Google Chrome」の安定（Stable）チャネルをアップデートした。現在、Windows/Mac環境にはv145.0.7632.75/76が、Linux環境にはv144.0.7559.75が展開中だ。

窓の杜からダウンロード

本リリースは修正パッチが提供される前に悪用が確認された脆弱性、いわゆるゼロデイ脆弱性に対処するための緊急アップデート。以下の問題が対処された。

- **CVE-2026-2441**：Use after free in CSS

深刻度の評価は、4段階中上から2番目の「High」。

●マイクロソフト2月の月例パッチ、古いIEコンポーネント・メモ帳等脆弱点修正

https://forest.watch.impress.co.jp/docs/news/2085116.html
https://msrc.microsoft.com/blog/2026/02/202602-security-update/
https://pc.watch.impress.co.jp/docs/news/2085270.html
https://news.mynavi.jp/article/20260211-4107339/

このニュースをザックリ言うと・・・

- 2月11日(日本時間)、マイクロソフトより、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 KB5077181(ビルド 26100.7840・26200.7840)および11 23H2 KB5075941(ビルド 22631.6649)となります。

- 修正された脆弱点のうちWord・Windowsシェルおよび古いInternet Explorer(IE)11のコンポーネントに対するもの3件が既に悪用を確認、これを含めた6件が攻撃手法公開済みとされています。

AUS便りからの所感

- 上記以外の脆弱点では、Azure関連3件を含む計5件について危険度が4段階中最高の「Critical」とされている他、Windows 11のメモ帳において、マークダウン(md拡張子)ファイル上の悪意のあるリンクからファイルを不正にダウンロードして実行する脆弱点(CVE-2026-20841)が修正されていることがトピックに挙げられています。

- 脆弱点修正以外にも、Windowsのセキュアブートのための証明書が6月下旬に順次失効するのに伴う新証明書への更新機構が今回のアップデートに含まれるとされ、PC等起動時に不正な処理が実行されることについても引き続き防御できるよう、確実にアップデートの適用が求められます。

Impress Watch

Microsoft、2026年2月の「Windows Update」を実施 ～ Word、Windows シェル、IEコンポで攻撃を確認

「メモ帳」にも脆弱性

樽井 秀人　2026年2月11日 09:40

米Microsoftは2月10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59件の脆弱性が新たに対処されている。

このうち、すでに悪用の事実が確認されているゼロデイ脆弱性は3件。「Word」やWindows シェル、「Internet Explorer」（MSHTML）に影響する。