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。

●Chrome「拡張スペルチェック」、Edge「Microsoftエディター」で入力した機密情報が外部に送信される恐れ…無効化で回避呼び掛け

https://gigazine.net/news/20220920-chrome-edge-expose-pii/
https://www.otto-js.com/news/article/chrome-and-edge-enhanced-spellcheck-features-expose-pii-even-your-passwords

このニュースをザックリ言うと･･･

- 9月16日(現地時間)、セキュリティベンダーのottoより、Chromeブラウザーの「拡張スペルチェック」機能およびEdgeブラウザーの「Microsoftエディター」機能において、機密情報を含む入力内容がGoogleやMicrosoftのサーバーに送信さ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。

- 注意喚起では、Chromeにて別のサイト上で「拡張スペルチェック」を有効化した直後、クラウドサービスのシークレットマネージャーにアクセスして機密情報を入力した際、入力された内容がGoogleのスペルチェック用サーバーに送信される様子、またパスワード入力欄においても「パスワードを表示する」オプションを有効にした場合に同様に送信される様子が画像・動画で挙げられています。

- 回避策として、Chromeでは拡張スペルチェックを、EdgeではMicrosoftエディターを無効化するよう呼び掛けられています。

AUS便りからの所感等

- 当初の注意喚起では、この問題がし得る主なWebサイトとして「Office 365」「Alibaba Cloud」「Google Cloud」「AWS」「LastPass」が挙げられていましたが、後日AWSとLastPassは対応が行われたとのことです。

- いずれのブラウザーにおいても、設定項目は「設定」→「言語」またはアドレスバーにabout://settings/languages の入力で表示され、Chromeの場合は「基本スペルチェック」を選択または「ウェブページにテキストを入力するときにスペルミスがないか選択する」を無効にする、Edgeの場合は「Microsoftエディター」の右にある「基本」を選択または「文書作成支援を使用する」を無効にすることにより、問題となる設定が無効になります。

- Chromeにおいて一時的に拡張スペルチェック機能を有効にしたいという場合、前述した画像のとおり「Google検索と同じスペルチェックが使用されます。ブラウザに入力したテキストはGoogleに送信されます。」といった警告が表示されるものの、一度有効化した後の無効化は手動で行う必要があることに注意が必要です。

- 今後Webサイト側で、問題となり得るページにおいて機能が無効化される設定(HTMLのspellcheck属性によりスペルチェックを無効化することが可能)が進むとともに、ブラウザー側でも当該機能の調整が行われることに期待したいところです。

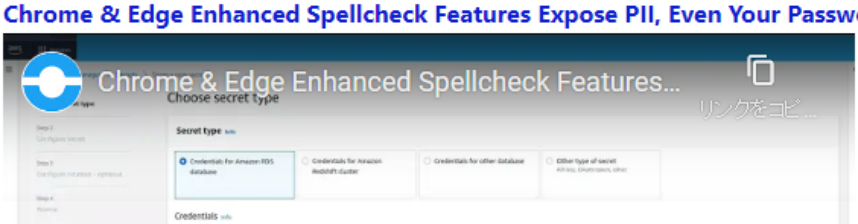
GIGAZINE

2022年09月20日 12時15分　セキュリティ

Google ChromeとMicrosoft Edgeで機密性の高い情報が拡張スペルチェック機能経由で外部サーバーに送信されている

Google ChromeやMicrosoft Edgeには、ユーザーの入力した単語が正しいスペルかどうかをサーバーのデータを用いてチェックする「拡張スペルチェック」機能があります。この「拡張スペルチェック」を利用したとき、基本的に入力フィールド内のすべての情報が外部サーバーに送信されていることがサイバーセキュリティ企業のottoにより指摘されています。「パスワードの表示」を行った場合は、パスワードすらも送信されるとのことです。

Chrome & Edge Enhanced Spellcheck Features Expose PII, Even Your Passwords - YouTube



●「Microsoft Teams」デスクトップアプリに認証トークンを平文で保持する脆弱性…ブラウザーからの使用呼び掛け

https://news.mynavi.jp/techplus/article/20220916-2456457/
https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/

このニュースをザックリ言うと･･･

- 9月13日(現地時間)、セキュリティベンダーのVectra社(以下・同社)より、ビデオ会議サービス「Microsoft Teams」のデスクトップアプリにおいて認証トークンを暗号化しない状態でPCに保存する脆弱性があるとして注意喚起が出されています。
- 脆弱性はWindows・Mac・Linux各OS向けのデスクトップアプリに共通して存在し、攻撃者は認証トークンや、多要素認証(MFA)をオンにしたユーザーアカウントに不正アクセスが可能とされています。
- 同社の研究者が既にMicrosoft(以下・MS)に連絡しているものの、「将来の製品リリースで対応予定(早急な修正の予定はない)」と回答されたとのことで、修正されるまでTeamsの利用はデスクトップアプリではなくブラウザーから行うよう呼び掛けています。

AUS便りからの所感

- Teamsデスクトップアプリには多くのアプリでの利用実績がある「Electron」フレームワークが使われていますが、同社ではElectronが暗号化等の機能を備えていないと指摘しています。
- 注意喚起では、PC上に侵入した攻撃者が脆弱性を突いて認証トークンを取り出すシナリオが挙げられており、外部からユーザーを悪意のあるサイトに誘導する等によって直接機密情報を奪取することは現時点では不可能とみられることから、MS側は速やかに対応を行わないと判断したと思われます。
- 他の脆弱性の悪用やマルウェアの感染等の経路でPCに侵入された場合を想定し、そこからTeamsアカウントの乗っ取り等が行われることを懸念するならば、注意喚起の通りデスクトップアプリの利用を控えブラウザーからの利用に切り替えることは有用でしょうし、一方でPCへの侵入はその他の様々な攻撃にも繋がることから、OS・アプリケーションさらには各種ハードウェアを制御するファームウェアを可能な限り最新に保ち、アンチウイルスやUTM等による侵入防御も万全に行う必要があるでしょう。

TECHR Powered by マイナビニュース

Microsoft Teamsアプリ、認証トークンを平文で保存 - ブラウザ版の利用を

2022/09/16 17:38　著者：後藤大地

Bleeping Computerは9月14日(米国時間)、「Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs」において、Microsoft TeamsのアプリがWindows、Linux、Macで認証トークンを平文で保存していると伝えた。セキュリティ研究者がMicrosoft Teamsのデスクトップアプリに、認証トークンや多要素認証(MFA: Multi-Factor Authentication)を有効にしたアカウントへ不正アクセスできる深刻な脆弱性があることを発見している。

セキュリティ研究者の調査によって、Windows、Linux、Mac用のMicrosoft Teamsデスクトップクライアントがユーザー認証トークンへのアクセスを保護せずに平文で保存していることが判明した。これにより、Microsoft Teamsがインストールされているシステムのローカルにアクセスできる攻撃者は、トークンを盗み出し、被害者のアカウントにログインするために悪用できるとされている。

● Windows 10 21H1、12月パッチをもってサポート終了… 21H2・22H2へのアップグレードを

https://forest.watch.impress.co.jp/docs/news/1440108.html
https://docs.microsoft.com/en-US/lifecycle/announcements/windows-10-21h1-end-of-servicing

このニュースをザックリ言うと･･･

- 9月15日(現地時間)、Microsoftより、Windows 10 バージョン 21H1のサポートが12月をもって終了するにあたっての告知ページが設置されています。
- 当該バージョンの月例セキュリティパッチは12月13日リリース予定のものが最後となり、以後当該バージョン内での更新は行われなくなります。
- 現時点での最新バージョンである21H2か、秋～冬にリリース予定の22H2へのアップグレードが強く推奨されます。

AUS便りからの所感

- Windows 10の「大型アップデート」は、2004より後、20H2・21H1・21H2がいずれも2004と殆ど中身を共有している小規模な更新であること(22H2も同様のものになるとの情報もあります)、4月に21H2が基本的に全てのPCに提供されるようになった(AUS便り2022/04/19号参照)ことから、万が一21H1以前でアップグレードを止めている場合は速やかに21H2へのアップグレードを進めることが肝要です。
- 一方で、Windows 10自体のサポート期限も2025年10月までとなっており、後継となるWindows 11が要求するスペックは今から5年ほど前にリリースされたPCでも満たされない可能性があるため、「PC 正常性チェック」の実行等を行い、11を実行するための最小システム要件を満たさないPCを洗い出し、それらのPCは無理に11を入れるのではなく、新しいPCへのリプレースを行うよう準備することもまた大事でしょう。

Impress Watch

「Windows 10 バージョン 21H1」のサービス終了まであと3カ月 ～Microsoftが注意喚起

2022年12月13日まで

樽井 秀人　2022年9月15日 09:00

「Windows 10 バージョン 21H1」のサポートが2022年12月13日で終了

「バージョン 21H1」の「Windows 10」は、2022年12月13日（米国時間、以下同）にサービス終了を迎える。米Microsoftは9月15日、公式ドキュメントサイトに告知ページを設置して注意喚起している。