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。

●県Webサイト掲載のExcelファイルに非表示のシート、個人情報366人分流出か

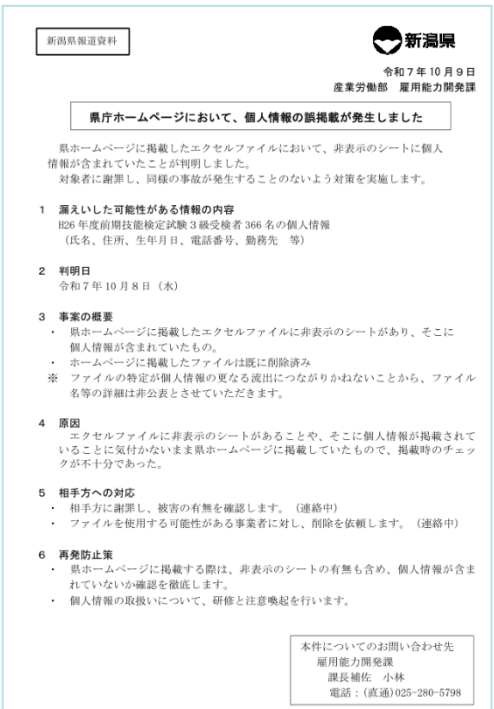
https://www.pref.niigata.lg.jp/sec/koyou/2510090001.html

このニュースをザックリ言うと･･･

- 10月9日(日本時間)、新潟県庁より、同県Webサイト上に掲載されたExcelファイルに個人情報が含まれていたと発表されました。
- 対象とされるのは、2014年度前期技能検定試験3級受検者366名分の氏名・住所・生年月日・電話番号および勤務先等となっています。
- 個人情報はExcelファイルで非表示になっていたシートに含まれていたとされ、同8日に判明、削除したとのことです。
- 同市では再発防止策として、Webサイトに掲載する際、非表示のシートの有無も含め、個人情報が含まれていないか確認を徹底すること等を挙げています。

AUS便りからの所感等

- 問題となったファイルについての詳細は公表されていませんが、関連する試験から、最長で10年間掲載されていた可能性もあります。
- Excelで非表示にしたシートは、ウィンドウ下部のシート一覧タブを右クリック→「再表示」から再表示することが可能ですが、非表示のシートが存在することを確認するには少なくともこの手段で「再表示」を選択可能かで判定する必要があり、これを意識していない限りは作業者でも見落とす恐れが高いでしょう(行列の非表示についても概ね同様のことが言えます)。
- 不特定多数へ公開するOfficeファイル等の用意にあたっては、個人情報等のチェックをくれぐれも全て目視のみで行わず、Officeが標準で持っている「ファイル」→「情報」→「問題のチェック」→「ドキュメント検査」により、シート・行列等非表示の内容・コメントその他各種情報をチェック・削除する、また同様の機能を提供するアドオンも検討する等、システムによる対策の実施を強く推奨致します。



新潟県報道資料

新潟県

令和７年10月９日
産業労働部　雇用能力開発課

県庁ホームページにおいて、個人情報の誤掲載が発生しました

県ホームページに掲載したエクセルファイルにおいて、非表示のシートに個人情報が含まれていたことが判明しました。
対象者に謝罪し、同様の事故が発生することのないよう対策を実施します。

1　漏えいした可能性がある情報の内容
H26年度前期技能検定試験３級受検者366名の個人情報
（氏名、住所、生年月日、電話番号、勤務先　等）

2　判明日
令和７年10月８日（水）

3　事案の概要
・県ホームページに掲載したエクセルファイルに非表示のシートがあり、そこに個人情報が含まれていたもの。
・ホームページに掲載したファイルは既に削除済み
※　ファイルの特定が個人情報の更なる流出につながりかねないことから、ファイル名等の詳細は非公表とさせていただきます。

4　原因
エクセルファイルに非表示のシートがあることや、そこに個人情報が掲載されていることに気付かないまま県ホームページに掲載していたもので、掲載時のチェックが不十分であった。

5　相手方への対応
・相手方に謝罪し、被害の有無を確認します。（連絡中）
・ファイルを使用する可能性がある事業者に対し、削除を依頼します。（連絡中）

6　再発防止策
・県ホームページに掲載する際は、非表示のシートの有無も含め、個人情報が含まれていないか確認を徹底します。
・個人情報の取扱いについて、研修と注意喚起を行います。

本件についてのお問い合わせ先
雇用能力開発課
課長補佐　小林
電話：(直通)025-280-5798

●Androidベースのデジタルフォトフレームに脆弱性…マルウェア拡散の恐れ

https://news.mynavi.jp/techplus/article/20251116-3666733/
https://www.bleepingcomputer.com/news/security/popular-android-based-photo-frames-download-malware-on-boot/
https://cybersecuritynews.com/android-photo-frames-app-downloads-malware/
https://www.quokka.io/blog/major-security-issues-digital-picture-frames

このニュースをザックリ言うと・・・

- 11月13日(現地時間)、モバイルセキュリティ企業のQuokka社より、Androidベースのデジタルフォトフレーム機器に複数の脆弱性が確認されていると報告されています。

- 同社が5月までに行った調査で判明したもので、機器で使用されているUhaleアプリケーションに10件近くの脆弱性が存在している他、起動直後に中国の不審なサーバーからスパイウェア・トロイの木馬をダウンロードして実行するものがあるとしています。

- Uhaleを搭載するデジタルフォトフレームは多数のブランドにおいて販売されており、Quokkaではユーザーに対しブランドを確認すること、該当するものは隔離し、他のPCが接続しているWi-Fiネットワークや公衆Wi-Fiに接続しないこと、アップデートの際も慎重に行うこと等を呼び掛けていますが、機器について使い続ける価値があるか判断の上、場合によっては破棄することが最も安全な選択肢となり得るとしています。

AUS便りからの所感

- Quokka社はUhaleを提供する中国ZEASN(Whale TV)社に対し本件について連絡をとろうとしたものの、回答を得られていないとしています。

- 報告を取り上げた米IT系メディアCyber Security Newsによれば、機器にはAndroid 6.0という非常に古いOSを使い、セキュリティ機能を無効化したものもあったとしています。

- デジタルフォトフレームにダウンロードされたマルウェアが、写真のアップロード等を行う管理用のスマホアプリを介してスマートフォン等に送り込まれることも考えられます。

- 一般論として、IoT機器においてもPCと同様ファームウェアの更新等を確実に行う、サポート切れとなった機種や、今回のような セキュリティアップデートを積極的に行う姿勢が見られない製品については、前述したように使用するリスク・コストを鑑みて破棄や別の機種に入れ替える、といった適切な管理が肝要です。


デジタルフォトフレームに重大な脆弱性、起動するとマルウェアを展開

掲載日 2025/11/16 16:29　著者：後藤大地

Bleeping Computerは11月13日(米国時間)、「Popular Android-based photo frames download malware on boot」において、一部のデジタルフォトフレームから重大な脆弱性が発見されたと報じた。一部の製品が起動時にマルウェアをダウンロードして実行するという。

BLEEPINGCOMPUTER

Popular Android-based photo frames download malware on boot

By Bill Toulas

Not all application allowlisting is created equal.

● Chromeのセキュリティアップデート…142.0.7444.175/.176への更新確認を

https://forest.watch.impress.co.jp/docs/news/2064032.html
https://forbesjapan.com/articles/detail/85308
https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

このニュースをザックリ言うと・・・

- 11月18日(日本時間)、Googleより、Chromeブラウザーのセキュリティアップデート142.0.7444.175/.176がリリースされました。

- JavaScriptエンジンV8の脆弱性2件(CVE-2025-13223, CVE-2025-13224)を修正するもので、特に1件(CVE-2025-13223)については既に悪用が確認されている「ゼロデイ脆弱性」とされています。

- Chromeブラウザーは自動更新に対応しており、また「ヘルプ」→「Google Chromeについて」(あるいはchrome://settings/help)でバージョン情報が確認できるとともに、手動でアップデートが可能です(更新の完了にはブラウザーの再起動が必要です)。

AUS便りからの所感

- 脆弱性の悪用により、ブラウザー上で任意のコードを実行する等、PCの乗っ取りに繋がる恐れがあるとみられ、攻撃者は悪意のあるWebサイトへの誘導や不正な広告の配信等で脆弱性を突くことが予想されます。

- ブラウザーを開いたまま、かつ「Google Chromeについて」をしばらく開いていない場合でも、更新・再起動を促すメッセージが表示されますが、アップデートのリリースから数日のタイムラグを置いて表示されることがあり、その間に脆弱性を悪用される可能性も考えられることから、できる限り毎日バージョンを確認し、最新バージョンに保つよう心掛けるべきでしょう。

- またブラウザーのバージョンが古く、更新されるまでの間に攻撃を受けることを避けられるよう、アンチウイルス・UTM等による防御も確実に行いましょう。


すぐに「Google Chrome」の更新を、スクリプトエンジン「V8」にゼロデイ脆弱性

Windows環境ではv142.0.7444.175/.176が展開中

樽井 秀人　2025年11月18日 07:45

米Googleは11月17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環境にはv142.0.7444.175/.176が、Mac環境にはv142.0.7444.176が、Linux環境にはv142.0.7444.175が展開中だ。

本リリースでは、以下の脆弱性が修正された。

- **CVE-2025-13223** : Type Confusion in V8
- **CVE-2025-13224** : Type Confusion in V8

深刻度の評価はいずれも「High」（4段階中上から2番目）にとどまるが、「CVE-2025-13223」はすでに悪用の報告がある。できるだけ早い更新が必要だ。