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。

●ソフトバンク契約者個人情報137,156件流出か…業務委託先にて情報持ち出し

https://www3.nhk.or.jp/news/html/20250611/k10014832201000.html
https://www.softbank.jp/corp/news/press/sbkk/2025/20250611_01/

このニュースをザックリ言うと･･･

- 6月11日(日本時間)、ソフトバンク社より、同社携帯電話サービスの一部契約者の個人情報が業務委託先から流出した可能性があると発表されました。

- 対象となるのは、「ソフトバンク」「ワイモバイル」個人契約者137,156件の氏名・住所・生年月日・電話番号・契約内容等とされています(クレジットカード情報・口座情報およびマイナンバー等は含まれていないとのことです)

- 業務委託先であるUFジャパン社(以下・UF社)の事務所において、その協力会社の元従業員Aが USBメモリーによる情報の持ち出しを行った可能性があったとしています。

- また、別の協力会社の従業員Bがクラウドサービスに情報をアップロードし、委託業務に携わっていない者から閲覧可能な状態となっていたことも発覚しています。

AUS便りからの所感等

- 元従業員Aは協力会社の退職後に拘らずUF社の事務所に不正に立ち入り、USBメモリーを情報管理端末に接続して情報の持ち出しを行っていたとされています。

- 在籍時に発行されていたユーザーアカウント等が有効なままで、端末へログインできた、あるいは他者がログイン中であった端末を不正に利用したのであれば、不要になったアカウントの無効化や、画面ロックの徹底が対策として肝要でしょう。

- 2023年にNTT西日本のグループ会社とNTTドコモにおいて相次いで発覚した個人情報持ち出し事案(のべ1,500万件近くの個人情報が被害)、遡れば2014年のベネッセの事案(最大3,504万件の個人情報が被害)等、今回と似通った事案にはそれぞれ本来意図しない形で個人情報を持ち出すことが可能だった様々な要因があり、そういった過去の事例、また今回においても後日出るであろう持ち出しに至る詳細な状況等の報告を参考とし、各種対策を打つべきです。

NHK

ソフトバンク 業務委託先から個人情報13万7000件余が流出か

2025年6月11日 19時02分　通信

通信大手のソフトバンクは、業務委託先の会社から携帯電話の契約者の氏名や住所、電話番号など13万7000件余りの個人情報が流出した可能性があると発表しました。会社は、委託先との契約を解除したうえで、警察に相談して今後の対応を検討するとしています。

ソフトバンクの発表によりますと、業務を委託していた「UFジャパン」という会社からソフトバンクとワイモバイルの契約者の氏名や住所、それに電話番号など13万7156件の個人情報が流出した可能性があるということです。

クレジットカードや口座番号などの情報は含まれていないということです。

● AIにメールを受信させて脆弱性を突く攻撃手法「Echoleak」、Copilotで修正

https://gigazine.net/news/20250612-echoleak-microsoft-copilot-zero-click-attack/
https://www.itmedia.co.jp/news/articles/2506/12/news074.html
https://www.aim.security/lp/aim-labs-echoleak-blogpost

このニュースをザックリ言うと･･･

- 6月11日(現地時間)、米Aim Security社より、AIシステムにユーザーの操作なしで攻撃を行う攻撃手法「Echoleak」について発表されました。

- 発表では、Microsoft 365 Copilotのメール・OneDrive・Teams等の保存データをAIからの回答のベースとする機能の脆弱性を突き、機密情報を外部に送信させることが可能だったとしています。

- 攻撃に際しては、細工したプロンプトをメールで受信させ、Webサイトのリンクのクリック等をAIに行わせる手口が取り上げられています。

- マイクロソフトでは既にAim社の報告を受け、Microsoft 365 Copilotの脆弱性を修正しているとのことです。

AUS便りからの所感

GIGAZINE

- ユーザーがメールのプレビューを行うことで攻撃が成立するケースは1990～2000年代におけるメーラーで度々報告されており、また主にメールサーバー側におけるアンチウイルス等のメールスキャン機能に脆弱性があり、不正なメールを送り付けるだけで悪意のあるコードをサーバー上で実行させられる事例も存在しています。

- 生成AIを中心としたAIブームにおいて、AIシステムの脆弱性の悪用により、機密情報が含まれている学習データを漏洩させる等の攻撃を行うことを多くの攻撃者が考えていることはたやすく予想でき、著作権で保護されている画像などを勝手に学習する等の問題と同様にセキュリティ上の問題も徹底して考慮され、対策が打たれることを期待したいものです。

●Microsoft等月例のセキュリティアップデート…Win11 24H2はパッチ差し替えも

https://forest.watch.impress.co.jp/docs/news/2021598.html
https://msrc.microsoft.com/blog/2025/06/202506-security-update/
https://forest.watch.impress.co.jp/docs/news/2021967.html
https://forest.watch.impress.co.jp/docs/news/2021596.html

このニュースをザックリ言うと･･･

- 6月11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 KB5060533(ビルド 19045.5865)、11 23H2 KB5060999(ビルド 22631.5472)および11 24H2 KB5063060(ビルド 26100.4351、6月12日リリース)等となります。

- Windows 11 24H2については、11日リリースのKB5060842(ビルド 26100.4349)が互換性の問題等で配信が段階的に行われる等の状況となり、12日リリースのKB5063060に差し替えられています(既にKB5060842がインストールされたPCには配信されない場合もある模様です)。

AUS便りからの所感

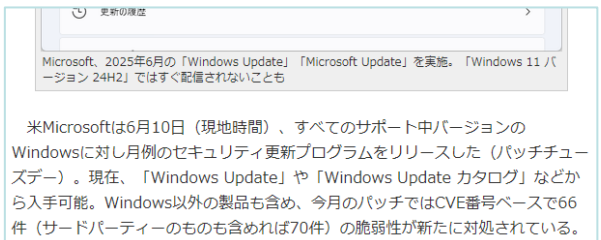
Impress Watch

- MSの月例アップデートでは1件の脆弱性が既に悪用を確認、1件が攻撃手法が公知となっている他、Office・リモートデスクトップサービス・ドメインコントローラー等10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。

- この他同11日にはAdobe社よりAcrobat・Acrobat Reader・InDesign等7製品について、Google社よりChromeブラウザーについて、それぞれセキュリティアップデートがリリースされています。

- システム管理者においては、MSの「パッチチューズデー(米国時間での第2火曜日にあたる)」を中心にソフトウェアベンダー各社が定期的(月例の他、隔月・四半期毎のものも)に行うアップデートを意識し、OS・ファームウェアないし各種アプリケーションのアップデートと、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ましょう。


Microsoft、2025年6月の「Windows Update」 ～ Windows 11 24H2ではすぐ配信されないことも
ゼロデイを含む66件の脆弱性を修正、「Microsoft Office」などに致命的な問題
樽井 秀人　2025年6月11日 09:56


Microsoft、2025年6月の「Windows Update」「Microsoft Update」を実施。「Windows 11 バージョン 24H2」ではすぐ配信されないことも

米Microsoftは6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66件（サードパーティーのものも含めれば70件）の脆弱性が新たに対処されている。