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。

● 12月の月例セキュリティアップデート、Microsoft・Adobe等発表

https://forest.watch.impress.co.jp/docs/news/2069934.html
https://msrc.microsoft.com/blog/2025/12/202512-security-update/
https://forest.watch.impress.co.jp/docs/news/2069940.html
https://forest.watch.impress.co.jp/docs/news/2070166.html

このニュースをザックリ言うと・・・

- 12月10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 11 24H2・25H2 KB5072033(ビルド 26100.7462・26200.7462)および11 23H2 KB5071417(ビルド 22631.6345)となり、修正された脆弱点のうちWindows・Windows PowerShell等の3件が既に悪用が確認ないし攻撃手法が公開済みとされ、またOffice・Outlookの3件について危険度が4段階中最高の「Critical」と評価されています。

- 同日にはAdobe社よりAcrobat(およびAcrobat Reader)・ColdFusion等5製品について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

- 攻撃手法が公開済みとされるWindows PowerShell 5.1での脆弱性(CVE-2025-54100)対策の一環として、「Invoke-WebRequest」コマンドレット実行時に警告プロンプトの表示が追加されており、一部スクリプトの実行時に注意が必要となっています(古いコンポーネントによるHTMLファイルの解析でスクリプトが実行される可能性を抑制するためとされます)。

- Windowsについては毎月下旬にもプレビューパッチがリリースされますが、今月は冬期休暇のため、10日リリースのアップデートが今年最後になるとのことです。

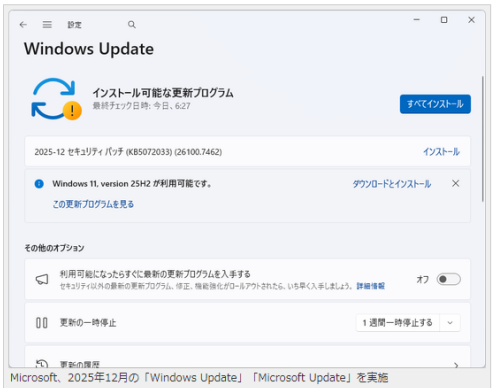
- MSを中心とした各社のアップデート集中日となっている「パッチチューズデー(米国時間での第2火曜日にあたる)」の他、例えばOracleは来年1月21日にJava等の四半期毎のアップデートを予定しており、このような定期的アップデートのスケジュールについて、特にシステム管理者においては忘れず意識し、OS・機器のファームウェアから各種アプリケーションに至るまで脆弱性への根本的対策としてのアップデートの適用を必須とし、加えてアンチウイルス・UTM等による多重防御策により、適用前の脆弱性への攻撃に備えることが肝要です。

Impress Watch

マイクロソフト、2025年12月の「Windows Update」を実施 ～「Office」に致命的な脆弱性

Jetbrains向け「GitHub Copilot」、「PowerShell」のゼロデイ脆弱性にも注意

樽井 秀人　2025年12月10日 08:50



Microsoft、2025年12月の「Windows Update」「Microsoft Update」を実施

米Microsoftは12月9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70件（サードパーティーも含む）の脆弱性が新たに対処されている。

●電話で答えたメールアドレスにフィッシングメール…「ボイスフィッシング詐欺」再発受け警察庁が注意喚起

https://www.itmedia.co.jp/news/articles/2512/05/news047.html
https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.12cpal.pdf

このニュースをザックリ言うと･･･

- 12月4日(日本時間)、警察庁「サイバー警察局便り」にて、いわゆる「ボイスフィッシング詐欺」が企業の法人口座をターゲットとして再発・急増しているとして注意喚起が出されています。

- 手口の一例として、銀行関係者を騙ってメールアドレスを聞き出し、そのアドレスにフィッシングサイトへのリンクが記載されたメールを送信、アクセス先で入力させたネットバンキングの認証情報を悪用して不正送金を行うものとなっています。

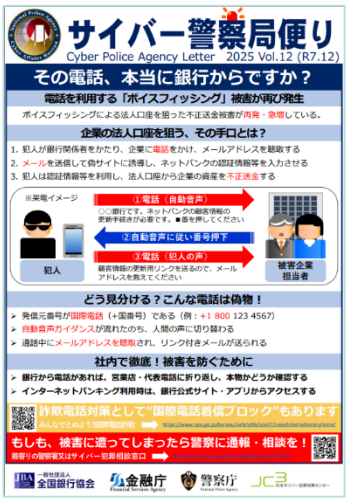
- 電話の特徴として、発信元番号が「+1 800 *** ****」等「+」で始まる国際電話である、自動音声ガイダンスの後に人間の声に切り替わるといった点も挙げられています。

AUS便りからの所感

- ボイスフィッシング詐欺は昨年秋以降に全国で事例が報告され、各銀行でネットバンキングでの即時振込を一時停止する所が相次ぎ、自動音声による案内や、電話・電子メール・SNS等で契約情報を訊ねることはないと呼びかける事態となっています。

- 警察庁では本物かどうか確認するために営業店の代表電話に折り返し電話をかけることを推奨しており、その際には安易にメールに記載された電話番号を信用せず、ネット上で本物の番号を検索する、また電話以外にもネットバンキングを利用する際にも予め本物の銀行サイトをブックマークに保存する、公式アプリからアクセスする等が有用です。

- また国際電話の着信を拒否する方法も取り上げられていますが、固定電話と携帯電話とでキャリア各社による提供、アプリによる提供等様々な方法があり、また携帯電話への海外からのSMSを拒否する方法もあるものの、正規のネットサービスが海外から送信するSMSを受信できなくなる可能性もあることに留意しながら検討すべきでしょう。



● Apacheに5件の脆弱点、セキュリティアップデート2.4.66リリース

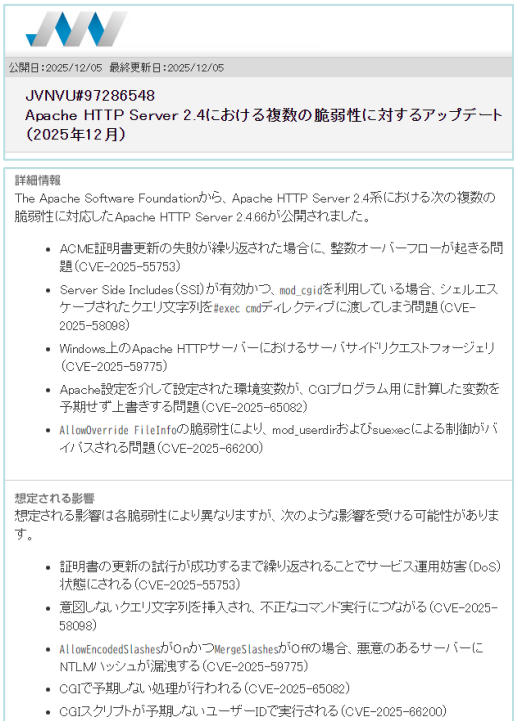
https://jvn.jp/vu/JVNVU97286548/index.html
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.66

このニュースをザックリ言うと･･･

- 12月5日(日本時間)、Apache Software Foundationより、Apache HTTP Server(以下・Apache)のセキュリティアップデート2.4.66がリリースされ、5件の脆弱点が修正されています。

- 脆弱点の多くはそれぞれ特定の環境やモジュールが有効な場合に限定されますが、サービス拒否(DoS)状態に陥る、想定外の内容あるいはユーザー権限によるコマンドが実行される等の可能性があるとしています。

- 12月11日現在、Linuxディストリビューション各種でまだアップデートはリリースされていない模様ですが、リリースが確認され次第、適用を推奨致します。


公開日:2025/12/05 最終更新日:2025/12/05

JVNVU#97286548
Apache HTTP Server 2.4における複数の脆弱性に対するアップデート(2025年12月)

詳細情報
The Apache Software Foundationから、Apache HTTP Server 2.4系における次の複数の脆弱性に対応したApache HTTP Server 2.4.66が公開されました。

- ACME証明書更新の失敗が繰り返された場合に、整数オーバーフローが起きる問題(CVE-2025-55753)
- Server Side Includes(SSI)が有効かつ、mod_cgidを利用している場合、シェルエスケープされたクエリ文字列を#exec cmdディレクティブに渡してしまう問題(CVE-2025-58098)
- Windows上のApache HTTPサーバーにおけるサーバサイドリクエストフォージェリ(CVE-2025-59775)
- Apache設定を介して設定された環境変数が、CGIプログラム用に計算した変数を予期せず上書きする問題(CVE-2025-65082)
- AllowOverride FileInfoの脆弱性により、mod_userdirおよびsuexecによる制御がバイパスされる問題(CVE-2025-66200)

想定される影響
想定される影響は各脆弱性により異なりますが、次のような影響を受ける可能性があります。

- 証明書の更新の試行が成功するまで繰り返されることでサービス運用妨害(DoS)状態にされる(CVE-2025-55753)
- 意図しないクエリ文字列を挿入され、不正なコマンド実行につながる(CVE-2025-58098)
- AllowEncodedSlashesがOnかつMergeSlashesがOffの場合、悪意のあるサーバーにNTLMハッシュが漏洩する(CVE-2025-59775)
- CGIで予期しない処理が行われる(CVE-2025-65082)
- CGIスクリプトが予期しないユーザーIDで実行される(CVE-2025-66200)

AUS便りからの所感

- Apacheでは不定期にセキュリティアップデートがリリースされていますが、2025年7月には2.4.64, 2.4.65の2回、2024年7月には2.4.60, 2.4.61, 2.4.62の3回と同じ月に複数回のリリースが行われています。

- 脆弱点のうち例えば「CVE-2025-58098」はSSI(Server Side Include)という古い機能とmod_cgid(mod_cgiは影響しないとのことです)との組合せによるものとされ、mod_include(SSIを提供)やmod_cgidを無効化することで回避することが期待できますが、このように使用していないモジュールを拙速に確認して無効化するよりは、Webサイト構築段階で必要最低限のモジュールのみ有効化するアプローチをとる方が安全でしょう。