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。

●「住民税納付」「引落し失敗」…PayPay悪用のフィッシング相次ぐ、不正送金被害の報告も

https://www.itmedia.co.jp/news/articles/2605/12/news143.html
https://www.antiphishing.jp/news/alert/rtax_20260511.html
https://did2memo.net/2026/05/10/sms-paypay-bank-hikiotoshi-shippai/
https://togetter.com/li/2696944
https://paypay.ne.jp/notice/20260515/s-01/

このニュースをザックリ言うと･･･

- 5月11日(日本時間)、フィッシング対策協議会より、住民税の納付依頼を騙るフィッシングメールに注意喚起が出されています。

- 挙げられているフィッシングメールの一例は、「【重要】令和8年度 住民税（第1期）納付のご案内」という件名で、「PayPayで今すぐ納付する」と記載されたリンクから、PayPayアプリを起動させて不正送金へ誘導するものとみられています。

- またX(旧Twitter)上では5月10日にPayPayやPayPay銀行を騙り「当月請求金額の口座引落ができませんでした」等とするSMSでのフィッシングが報告、同13日にはあるユーザーから、PayPayアカウントに紐づけていたクレジットカードおよび銀行口座から数百万円の不正なチャージ・出金を行われたとする被害報告も出ています。

- PayPay社からも、5月15日に「クレジットカードの請求や通信料金、税金等が未払い・未納である」といったメール・SMSでPayPay残高を送付させようとする手口について注意喚起が出されています。

AUS便りからの所感等

- フィッシング対策協議会では4月にもPayPayアプリでの支払いへ誘導する事例の注意喚起を行っており、また今回取り上げている事例も含め、フィッシング用URLから誘導された先では「https://qr.paypay.ne.jp/p2p01_●●●●」という正規のURLも用いているとしています。

- PayPay社では「企業や団体へのお支払いに、送る・受け取る機能は利用されていません」とし、またカード情報・銀行口座情報等が不正利用された場合の補償制度も用意されている一方、PayPay残高をユーザー自身で送った場合は補償制度の対象外となるとしています。

- PayPayでの支払いやチャージ等については利用可能額の制限が設定可能です(制限解除や制限額引き上げの際は指紋認証・PIN入力等が要求されます)が、これを設定していない場合、紐づけた銀行口座やクレジットカードから多額のチャージを行われ、外部に不正送金される恐れがあります。

- 他にもPayPayにはいくつかのセキュリティ機構が提供されており、安全のため一通り設定を行うことが肝要ですが、それでもPayPayアプリ上で送金先等を提示され、あとは送金ボタンをタップすると資金流出が発生してしまう状態まで一気に誘導される可能性があり、PayPay社が推奨するとおり、心当たりのない請求・督促のメールやSMSに対しては、リンクやボタンのクリックを決して行わないよう慎重に行動するべきでしょう。

ITmedia NEWS

「住民税の納付」装う詐欺メール拡散　PayPayで送金迫る手口、フィッシング対策協議会が警戒呼び掛け

2026年05月12日 20時10分 公開　[梅林日奈子，ITmedia]

住民税の納付依頼を装うフィッシングメールについて、フィッシング対策協議会が注意喚起している。5月11日に公開した手口には、コード決済サービス「PayPay」のURLを悪用し、受信者を偽のWebサイトに誘導するメールを紹介している。

確認されたメールの件名には「住民税の納付依頼」や「納付期限が近づいています」といった文言が記載されている。本文では、納税額やPayPayへの誘導リンクが記されており、「期限までに納付が確認できない場合、法的措置を執る」といった内容が記載されている。

●「パッチチューズデー」MSが5月の月例セキュリティアップデート…一方でExchange Serverの未対策の脆弱点発表

https://forest.watch.impress.co.jp/docs/news/2108062.html
https://www.microsoft.com/en-us/msrc/blog/2026/05/202605-security-update
https://jpmessaging.github.io/blog/addressing-exchange-server-may-2026-vulnerability-cve-2026-42897/

このニュースをザックリ言うと･･･

－5月13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 KB5089549(ビルド 26100.8457・26200.8457)および11 26H1(一部機種で使用) KB5089548(ビルド 28000.2113)等となります。

－サードパーティー製含め138件の脆弱点が修正、うち危険度が4段階中最高の「Critical」と評価されているものが30件とされています。

AUS便りからの所感

－Criticalとされる脆弱点はOffice・Word等の他、Windows 11およびServer 2025のDNSクライアントで、悪意のあるDNS応答を受けることによりPCを乗っ取られる可能性があるもの(CVE-2026-41096)が報告されています。

－一方で同社からは、Exchange Serverに今回修正されていないクロスサイトスクリプティング(XSS)の脆弱点(CVE-2026-42897)が存在することも発表されており、Exchange Outlook Web Access(OWA)で悪意のあるメールを開いた場合、不正なスクリプトをブラウザー上で実行される可能性があるとされ、回避策が提示されています(Exchange Onlineは影響を受けないとのことです)。

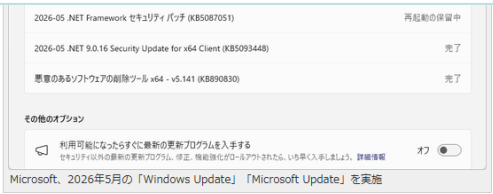
－MSあるいは各社からのアップデートが集中する毎月の「パッチチューズデー(米国時間での第2火曜日にあたる)」において、OS・機器のファームウェアから各種アプリケーションに至るまでアップデートや回避策の適用により、脆弱性への根本的対策を行うこと、加えて適用前あるいはパッチが出ていない脆弱性への攻撃に備え、アンチウイルス・UTM等による多重防御策も確実に行うようにしてください。

Impress Watch

Microsoft、2026年5月の「Windows Update」を実施 ～138件中30件は"緊急"の脆弱性

OSや「Azure」製品、「Copilot」、「Office」、「.NET」などに影響

樽井 秀人　2026年5月13日 09:24



Microsoft、2026年5月の「Windows Update」「Microsoft Update」を実施

米Microsoftは5月12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138件の脆弱性が新たに対処されている。

● Oracle社製品のセキュリティアップデートを四半期から月例へ…5月29日リリース予告

https://blogs.oracle.com/oracle4engineer/ja-update-monthly-critical-security-patch-updates-cspus-begin-may-28-2026
https://blogs.oracle.com/oracle4engineer/ja-accelerating-vulnerability-detection-and-response-at-oracle

このニュースをザックリ言うと･･･

－5月5日(日本時間・以下同様)、Oracle社より、同社製品について、四半期に一度のアップデート(Critical Patch Updates, CPU)に加えて月例のセキュリティアップデート(Critical Security Patch Updates, CSPU)を実施することが発表されています。

－前回の四半期アップデートは4月22日に行われ、次回は7月22日に予定されていますが、加えて重大な脆弱点への優先的な対応として月例リリースを行うとしています。

－月例リリースは初回が5月29日に行われること、以後は6月17日・8月19日と、第3火曜日(米国時間)のリリース予定がアナウンスされています。

AUS便りからの所感

－Oracle社は4月30日、脆弱性の検査・脆弱点の検出がAIにより非常に迅速化されている状況に触れ、同社でもAnthropic社の「Claude Mythos」等によって製品の検査を行っていることに言及しています。

－具体的に同社のどの製品において月例リリースが行われるかの発表はまだなく、例えばJava(JDK)についても現時点では四半期アップデートの予定のみが示されています。

－特にシステム管理者においては、初回の月例リリース時あるいはそれ以前の情報の発表でどの製品が影響を受けるかを把握すること、そしてOracle社以外の製品も含めたアップデートのリリーススケジュールおよびその追加・変更について忘れずに意識し、毎回のリリース時に可能な限り早く適用できる体制を整えることが重要です。

ORACLE

更新情報: 月次のCritical Security Patch Updates (CSPUs)を2026年5月28日より開始

May 6, 2026 | 1 minute read

Noriyuki Tajima

この記事はIntegrated Cyber Center (ICC)によるUpdate: Monthly Critical Security Patch Updates (CSPUs) Begin May 28, 2026を日本語に翻訳したものです。

2026年5月6日

先日公開した記事 Oracleにおける脆弱性の検出と対応の迅速化に続き、月次のCritical Security Patch Updates (CSPUs)の提供開始日と頻度を発表します。

2026年5月28日より、Oracleは毎月Critical Security Patch Update(CSPU)を提供します。CSPUは、重大な脆弱性に対する修正を、より小規模で的を絞った形式で提供するものであり、これによりお客様は、次の四半期リリースを待つことなく、優先度の高い問題に対処できるようになります。

CSPUは、Oracleの既存の四半期ごとのCritical Patch Updates (CPU)を補完するものです。

- 月次CSPUは、重大な問題に対するタイムリーで優先度の高い修正を提供します
- 四半期ごとのCPUは引き続き累積的なものであり、以前のCSPUでリリースされたすべての修正が含まれます

このアプローチにより、お客様管理環境のお客様は、次回の四半期サイクルを待たずに重大な修正をより早く適用することで、リスクを軽減することができます。