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。

●WordPressに危険度の高い脆弱点「wp2shell」報告…対象バージョンは必ずアップデート確認を

https://forest.watch.impress.co.jp/docs/news/2126337.html
https://www.ipa.go.jp/security/security-alert/2026/alert20260722.html
https://slcyber.io/research-center/wp2shell-pre-authentication-rce-in-wordpress-core
https://piyolog.hatenadiary.jp/entry/2026/07/19/181822

このニュースをザックリ言うと･･･

- 7月18日(日本時間)、英Searchlight Cyber社より、WordPressにおいて危険度の高い脆弱点「wp2shell」を発見したとして注意喚起が出されています。

- wp2shellは2件の脆弱点(CVE-2026-63030, CVE-2026-60137)からなり、両方の脆弱点の影響を受けるWordPress 6.9.0～6.9.4・7.0.0～7.0.1において、認証されていない攻撃者にサーバー上で任意のコードを実行される恐れがあるとしています。

- wp2shellは、WordPressをインストールした初期状態で、何らかのプラグインをインストールしていない状態であっても、また攻撃者がWordPressにログインしている必要もなく、サーバーの乗っ取りが可能になるとされる、極めて危険度の高い脆弱点とされています。

- 既にWordPressのセキュリティアップデート6.9.5・7.0.2がリリースされており、IPA等からも、自動更新等で最新バージョンに更新されているか確認すること、されていない場合には手動で更新するよう検討することを呼び掛けています。

AUS便りからの所感等

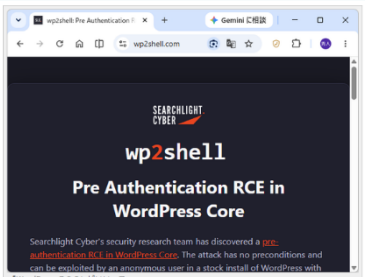
- REST APIのバッチ処理における脆弱点(CVE-2026-63030)と、WP_Queryの一部パラメータにおけるSQLインジェクションの脆弱点(CVE-2026-60137)の両方を満たす必要があるとされますが、6.8系(6.8.0～6.8.4)においても後者の脆弱点について影響を受けるとされ、セキュリティアップデート6.8.5がリリースされています。

- WordPressでは各種プラグインにおいても日々何らかの脆弱点が報告されており、例えばWordPress向けセキュリティプラグイン「Wordfence」の提供元からは、「Everest Forms Pro」(AUS便り 2026/06/18号参照)や「Gravity SMTP」等の脆弱点への攻撃が確認されているとする注意喚起が出ていました。

- WordPressを使用しているWebサイトの管理者においては、WordPress本体および使用しているプラグインについて随時セキュリティ情報を収集、特に意図的に自動更新していないものがあれば定期的に管理画面で各種アップデートの有無を確認すること、可能な限り前述したWordfenceをはじめとしたセキュリティ関連のプラグインないしWAFをも導入し、何重にもセキュリティを固めることが肝要です。

Impress Watch

「WordPress」に致命的脆弱性、未認証・条件なしで乗っ取れる ～CVSS 3.1で「9.8」
対策版の「WordPress 7.0.2」などが公開
樽井 秀人　2026年7月21日 11:15



「WordPress 7.0.2」がリリース

人気のブログシステム「WordPress」で、未認証でもリモートから任意コードを実行できてしまう致命的な脆弱性が発見された。この攻撃手法は「wp2shell」と呼ばれており、すでに概念実証（PoC）コードも存在する。「WordPress」の開発チームは7月17日付けで修正バージョンをリリースしている。

「wp2shell」は、以下の2つの脆弱性を組み合わせた攻撃手法。この手法を発見したSearchlight CyberのAdam Kues氏によると、事前に必要な条件は一切なく、プラグインをなにも導入していない状態の「WordPress」サイトでも匿名で悪用できてしまうという。

● 6月度フィッシング報告件数は72,370件…下旬に報告等急減

https://www.antiphishing.jp/report/monthly/202606.html

このニュースをザックリ言うと・・・

－7月16日(日本時間)、フィッシング対策協議会より、6月に寄せられたフィッシング報告状況が発表されました。

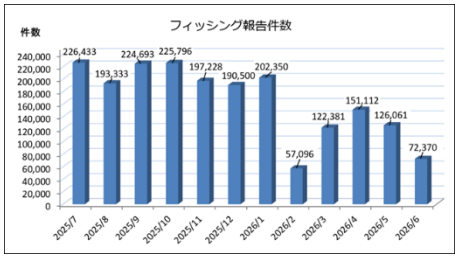
－6月度の報告件数は72,730件で、5月度(https://www.antiphishing.jp/report/monthly/202605.html)の126,061件から53,691件減少しています。

－悪用されたブランド件数は98件で5月度(112件)から14件減少、最も報告が多かったブランドはAmazonが約24.0%、次いでVISA(約11.8%)、Apple(約11.6%)、三井住友カード、NTTドコモと合わせて約55.0%、さらに1,000件以上報告された15ブランドまで含めると約74.3%となっています。

AUS便りからの所感

－月間の報告件数は急減をみせた2月度(57,096件)以来の10万件切りとなっており、また日々の報告件数及び調査用メールアドレス宛てへのフィッシングメール着信件数については、15日頃から25日頃まで上昇を見せた後は月末まで減少しています。

フィッシング対策協議会
Council of Anti-Phishing Japan



－フィッシングメールについても、4・5月まで多くの割合を占めていた中国からの発信が6月2日・3日頃をピークに減少、中旬以降はGoogle Cloudを中心とした米国のクラウドサービスからの発信がほとんどとされ、またPTRレコード(IPアドレスからの逆引き)設定のないIPアドレスからの発信も約32.8%と減少しています。

－またフィッシングサイトについては、モバイル回線以外のアクセス元では閲覧できないサイトが増加し、稼働確認や停止調整の回避を試みている可能性が2月度以降報告されており、こういった調査・作業のための固定回線からのアクセスの他、PCからアクセスする一般ユーザーについてもターゲットとせず回避しているケースも多々あるとみられます(この手の不審なサイトでは、検索エンジンからアクセスしてきた場合にのみ機能し、直接アクセスする場合は表示されないというケースも以前から珍しくありません)。

－フィッシングのトレンドにおいて、KDDIのISP向けメールシステムから流出したアカウント情報(AUS便り 2026/06/26号参照)を悪用したとみられるフィッシングの報告が急増したこと等に言及されており、対象となったユーザーにおいてはISPの呼び掛けに従って適宜パスワード変更等を行った上で、フィッシングの手口(どこを騙るか、どんな文面のメールやSMSを送るか、最終的な目的は何か)について十分に把握し、毎月のフィッシング報告の「利用者のみなさまへ」に記載された各種対策の実施をはじめ、慎重な行動を心掛けましょう。

●7-Zipに任意のコード実行の脆弱点…6月リリースの26.02で対策済み

https://forest.watch.impress.co.jp/docs/news/2125686.html
https://www.zerodayinitiative.com/advisories/ZDI-26-444/

このニュースをザックリ言うと・・・

－7月15日(現地時間)、脆弱点発見コミュニティ「Zero Day Initiative(以下・ZDI)」より、アーカイブ作成ソフト「7-Zip」に脆弱点(CVE-2026-14266)が存在すると発表されました。

－脆弱性はXZ圧縮形式のファイルを展開する機能に存在し、細工されたファイルを開くことにより、任意のコードをPC上で実行される恐れがあるとされています。

－脆弱性は6月にZDIから7-Zipの開発者へ報告、同25日にリリースされた26.02で修正されたとしており、ユーザーに対しアップデートが推奨されています。

AUS便りからの所感

Impress Watch

－本来はローカルに保存した悪意のあるファイルを開くことで発生する脆弱性ですが、メールに添付およびWebからダウンロードさせる攻撃が予想されるためか、ZDI等では本件を「リモートからの」コード実行の脆弱性としています。

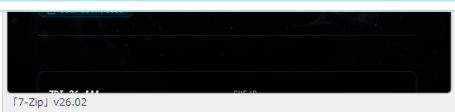
－XZ形式は主にLinux向けの「xz」「tar.xz」圧縮ファイルとして用いられることが多いですが、7-Zipでもこれらの拡張子のファイルに関連付けることが可能な他、悪意のあるファイルを「.7z」拡張子に偽装することも考えられ、7-Zipがこれを開いた場合、拡張子と圧縮形式との齟齬を無視して圧縮ファイルを展開しようとすることに注意が必要です。

－7-Zipには自動更新機能がなく、アップデートのリリース時に通知されないことに注意し、ヘルプからバージョン情報を確認の上、「www.7-zip.org」ボタンをクリックして公式サイト(https://www.7-zip.org/)からダウンロードを行うのが安全でしょう(サーチエンジンで「7-zip」で検索した場合、「7-zip.opensource.jp」のような公認の日本語サイトとは異なる偽サイトが広告等で表示される可能性があることに注意が必要です)。

「7-Zip 26.02」で解決された脆弱性は任意コード実行につながるおそれ ～ZDIが公表

オープンソースの解凍・圧縮ソフト

椿井 秀人　2026年7月16日 15:16



「7-Zip 26.02」で修正された脆弱性はヒープベースのバッファオーバーフローで、リモートから任意のコードを実行できる可能性があるとのこと。「Zero Day Initiative」（ZDI）が7月15日（米国時間）、セキュリティアドバイザリを公開した。

窓の杜からダウンロード

アドバイザリによると、本脆弱性のCVE番号は「CVE-2026-14266」。XZ形式の圧縮ファイルを扱う際のチャンク（大きなデータを扱いやすいように小分けしたブロック）データの処理に問題があり、メモリ破損を引き起こす可能性がある。悪意のあるWebページを開かせたり、細工を施したXZファイルを開かせるといったユーザー操作は必要だが、当該ユーザーの権限で任意のコードを実行できる可能性がある。