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。

●7-ZipにDoS攻撃の脆弱性…最新バージョン25.00に更新を

https://forest.watch.impress.co.jp/docs/news/2032783.html
https://securitylab.github.com/advisories/GHSL-2025-058_7-Zip/

このニュースをザックリ言うと・・・

- 7月17日(現地時間)、米GitHub社より、アーカイブ作成・解凍ソフト「7-Zip」に存在する脆弱性(CVE-2025-53816)について注意喚起が出されています。

- 脆弱性は「RAR5」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、バッファオーバーフローが発生し、DoS攻撃を仕掛けられる恐れがあるとされています。

- 脆弱性は7-Zipバージョン24.09で確認、4月に7-Zipの開発者へ報告されており、7月にリリースされた最新バージョン25.00で修正済みとのことで、ユーザーに対しアップデートが呼び掛けられています。

AUS便りからの所感等

- RAR5形式は、7-Zipと同じアーカイブ作成ソフト「WinRAR」で作成可能な圧縮形式で、7-Zipでも2015年リリースの15.06 betaから解凍にのみ対応しています。

- CVE-2025-53816はローカルからの攻撃とされていますが、悪意のあるRAR5形式のファイルをメールへの添付ファイルや不審なWebサイトからダウンロードさせる受動的攻撃のシナリオが考えられ、またより7-Zipでファイルを開く確率を上げるため、RAR5形式本来の「.rar」拡張子ではなく「.7z」拡張子を付与する可能性があります(アンチウイルス等でこのような拡張子の偽装に対し警告が出るケースもあります)。

- 根本的な対策のためには最新バージョンへのアップデートが必要ですが、7-Zipのような現時点で自動更新機能・アップデートリリース時の通知機能がないソフトウェアについては古いバージョンが使い続けられる可能性があり、アップデートのリリース情報を随時収集しつつ、各種ソフトウェアを含め最新のバージョンに保ち続けることを意識すること、並行して悪意のあるファイルの受信・ダウンロードを食い止めるためアンチウイルスやUTMによる防御も怠りなく実施することが重要となります。

- 前述の理由から、7-Zipの更新には通常ユーザー自身がインストーラーを入手することになりますが、サーチエンジンで「7-zip」で検索した場合に、不正な広告で表示されたサイトから偽のインストーラーを掴まされる恐れもあり、その意味でもアンチウイルス・UTMによる防御を行うとともに、7-Zipのバージョン情報から表示される公式サイト(https://www.7-zip.org/)にアクセスすることを心掛けましょう。

Impress Watch

解凍・圧縮ソフト「7-Zip」にヒープバッファーオーバーフローの脆弱性、GitHubが報告

修正版への更新を

樽井 秀人　2025年7月22日 00:10

GitHub Security Labのアナウンス

米GitHubのセキュリティチーム「GitHub Security Lab」（GHSL）は7月17日（現地時間）、解凍・圧縮ソフト「7-Zip」でヒープバッファーオーバーフローの脆弱性（CVE-2025-53816）を発見したことを明らかにした。「RAR5」書庫ファイルの処理に問題があり、メモリ破壊やサービス拒否につながる可能性があるという。

本脆弱性は、「7-Zip 24.09」の「RAR5」のデコーダーで発見された。このデコーダーは破損したアイテムをゼロで埋めて修正しようと試みるが、上書きするバイト数を外部から制御できるため、確保されたバッファを越えてゼロが書き込めてしまう。任意のコード実行につながる可能性は低いが、メモリを破壊してアプリを応答不能に陥らせることができる（サービス拒否）。

●米マクドナルドの求人サイト、管理画面に簡単なID・パスワード使用…約6,400万件の求人情報にアクセス可能な状態

https://gigazine.net/news/20250710-mcdonalds-job-hire-leak/
https://wired.jp/article/mcdonalds-ai-hiring-chat-bot-paradoxai/
https://ian.sh/mcdonalds

このニュースをザックリ言うと･･･

- 7月9日(現地時間)、セキュリティ研究家のIan Carroll・Sam Curry両氏より、米マクドナルド社への求人者情報6,400万件にアクセス可能だったと発表されました。
- 同社の求人サイト「McHire」で使用されているAIボット「Olivia」について両氏が調査していた過程で、管理画面においてID・パスワードの両方に「123456」を入力することでログイン可能な状態だったことを発見したとしています。
- またログイン後の管理画面において、応募者とOliviaとの会話内容や、応募者の氏名・メールアドレス・電話番号・住所等にアクセス可能だったとしています。
- 6月30日に両氏がマクドナルド社へ報告を行ったところ、Oliviaを運営するParadox.ai社から連絡があり、約2時間後には前述のID・パスワードでログインできなくなったとのことです。

AUS便りからの所感

- Carrorl・Curry両氏は、Oliviaに対するセキュリティ突破ができないか調査をしていた際にParadox.ai社が使う管理画面へのリンクを見つけたとしています。
- ID・パスワード「123456」は初期状態のアカウント情報であり、管理者が変更していなかったことが原因としている一方、Paradox.ai社では両氏以外の第三者から当該アカウントへのアクセスの形跡はなかったとしています。
- 初期のアカウントのパスワードに「admin」等が使われているケースはルーター・NAS・複合機等のネットワーク機器においてもよく見られ、これを変更していなかったり、さらに外部から管理画面にアクセス可能だったりする機器は格好のターゲットとなり得るため、パスワード(可能であればIDも)を推測されにくいものに変更することは言うまでもなく、近年はそれに留まらず多要素認証の設定も強く推奨されます。

● Apache HTTP ServerとDNSサーバーBIND・Unbound、相次いでセキュリティアップデートリリース

https://jvn.jp/vu/JVNVU91930855/
https://jprs.jp/tech/security/2025-07-17-bind9-vuln-serve-stale.html
https://jprs.jp/tech/security/2025-07-18-unbound.html

このニュースをザックリ言うと･･･

- 7月11日(日本時間)、Apache Software Foundationより、「Apache HTTP Server(以下・Apache)」の最新バージョン2.4.64がリリースされ、8件の脆弱性が修正されています。
- 同17日にはISCより、DNSサーバー「BIND」最新バージョン9.20.11がリリースされ、脆弱性1件(CVE-2025-40777)が修正されています。
- さらに同18日にはキャッシュDNSサーバー「Unbound」の脆弱性1件(CVE-2025-5994)を修正したバージョン1.23.1がリリースされています。

AUS便りからの所感

- BINDの脆弱性は2件発表されており、前述したCVE-2025-40777は9.20系にのみ影響(9.18系以前は影響しない)、残る1件(CVE-2025-40776)も一般に使用されないバージョンでのみ影響するものとされます。
- 一方でUnboundの脆弱性CVE-2025-5994はUnbound以外の複数のプロダクトにも影響するものとされ、また脆弱性が存在する箇所から、BINDのCVE-2025-40776と同様のものである可能性が考えられます。
- 7月22日時点でLinuxディストリビューションのうちRHEL系(Almalinux・Rocky Linux等)については、BINDはいずれの脆弱性も影響しないバージョンを使用していますが、Apache・Unboundのパッケージはまだ更新されておらず、更新され次第速やかに適用する体制を準備することを推奨致します。