— AUS（アルテミス・ユーザ・サポート）便り 2024/11/28号 —
https://www.artemis-jp.com

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に任意のコード実行の脆弱性、バージョン24.07で修正済み

https://forest.watch.impress.co.jp/docs/news/1642421.html
https://securityonline.info/cve-2024-11477-7-zip-vulnerability-allows-remote-code-execution-update-now/
https://www.zerodayinitiative.com/advisories/ZDI-24-1532/

このニュースをザックリ言うと・・・

- 11月20日(現地時間)、トレンドマイクロ社が運営する脆弱性発見コミュニティ「Zero Day Initiative(以下・ZDI)」より、アーカイブ作成ソフト「7-Zip」に脆弱性(CVE-2024-11477)が存在すると発表されました。

- 脆弱性は「Zstandard(以下・zstd)」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、同月にリリースされた24.07で修正されたとしており、ユーザーに対し現時点で最新バージョンである24.08へのアップデートが推奨されています。

AUS便りからの所感等

- 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おり、zstd形式で圧縮した悪意のあるファイルを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とみられます。

- また、悪意のあるファイルを7-Zipに関連付けられる「.7z」拡張子に偽装することが考えられ、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(一方で7-Zipの設定次第ではzstd形式で通常使われる「.zst」「.zstd」拡張子にも関連付けられるため、こちらも油断は禁物です)。

- 根本的な対策として7-Zip 24.07以降へのアップデートが必要不可欠ですが、現時点で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ため、インストールしている場合はバージョンを確認の上、公式サイト(https://www.7-zip.org/)か信頼できるミラーサイトからダウンロードを行うよう心掛けましょう(サーチエンジンで「7-zip」で検索した場合、広告として偽サイトが表示される可能性があります)。

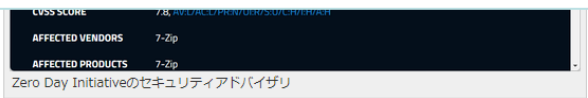
- zstd形式は1月リリースの7-Zip 24.01で新たに対応したもので、脆弱性もバージョン24.01～24.06に影響するとみられますが、これよりさらに前のバージョン(23.01以前)には恐らく影響しないからと言って、そのような古いバージョンを使い続けるのではなく、アップデートのリリース情報を随時収集しつつ、各種ソフトウェアを含め最新のバージョンに保ち続けること、並行して悪意のあるファイルの受信・ダウンロードを食い止めるためアンチウイルスやUTMによる防御も怠りなく実施することが重要です。

Impress Watch

解凍・圧縮ツール「7-Zip」にリモートコード実行の脆弱性

「7-Zip 24.07」以降へのアップデートが必要

樽井 秀人　2024年11月26日 08:23



Zero Day Initiativeのセキュリティアドバイザリ

解凍・圧縮ソフト「7-Zip」に、リモートコード実行の脆弱性が発見された。6月19日にリリースされた「7-Zip 24.07」以降へのアップデートが必要だ。

この脆弱性は、「Zstandard」における解凍（展開）処理の実装に起因する。ユーザーから提供されるデータを適切に検証しておらず、細工を施すことでメモリへ書き込む前に整数アンダーフローが発生させることが可能。任意のコードを現在のプロセスコンテキストで実行できるようになる。

問題はTrend Microのセキュリティ部門から6月12日に開発チームへ報告され、ほどなく修正された。両者の調整の上、11月20日にセキュリティアドバイザリが公開されている。深刻度の評価は、CVSSの基本値で「7.8」。できるだけ早い対処が必要だ。

●10月度フィッシング報告件数は181,443件、過去最多の7月度を凌ぐ

https://www.antiphishing.jp/report/monthly/202410.html

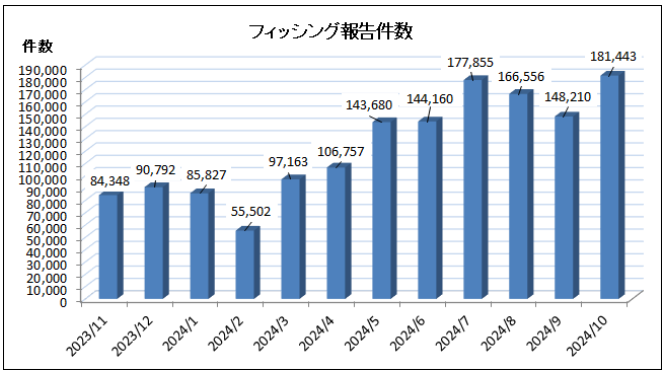
このニュースをザックリ言うと･･･

- 11月22日(日本時間)、フィッシング対策協議会より、10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。
- 10月度の報告件数は181,443件で、9月度(https://www.antiphishing.jp/report/monthly/202409.html)の148,210件から33,233件増加しています。
- フィッシングサイトのURL件数は71,367件で9月度(49,519件)から21,848件増加、悪用されたブランド件数は88件で9月度(79件)から9件増加となっています。
- Amazonを騙るフィッシングの割合は全体の約26.8%となり、次いで10,000件以上の報告を受けたヤマト運輸、東京電力、JCB、プロミスと合わせて約62.6%、さらに1,000件以上報告された23ブランドまで含めると約96.7%を占めたとのことです。

AUS便りからの所感

- 報告件数は、過去最多だった7月度の177,855件より3,588件多く、今後も急激な増減こそあれ、14万件台超の水準を維持するとみられます。
- フィッシングサイトのURL件数も9月度の一時的な減少を経て、過去最多だった8月度の85,768件に次いでおり、また使用されるTLD(トップレベルドメイン名)の割合は .com(約44.0%)、.cn(約37.6%)が依然突出していますが、5月度以降10%を超えているのはこの2つだけとなっています。
- 同協議会からは10月に特に警戒すべき6つのブランドに関するフィッシングへの注意喚起が出た(https://www.antiphishing.jp/news/alert/)他、日本データ通信協会の迷惑メール相談センターからも日々10～20件のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、利用しているサービスについて不審なメールを受信した際はこういった情報やX等ソーシャルネットワークでの報告と照合するとともに、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする等、慎重に行動することを日々心掛けましょう。

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



●福島県警のメールサーバー、スパムメール送信の踏み台にされる

https://nordot.app/1234115335722385432
https://www.minyu-net.com/news/detail/20241127102230299O7

このニュースをザックリ言うと･･･

- 11月26日(日本時間)、福島県警察本部(以下・県警)より、県警のメールサーバーが海外からのメール不正送信の踏み台にされたと発表されました。
- 悪用されたのは広報活動や企業とのやりとりに使う外部向けメールサーバーとされ、同26日の午前6時～午後2時頃にかけて、「Notice」等の件名、英文からなる約5万件のメールが国内外の不特定多数へ送信されたとしています。
- 不審なメール送信の発覚を受けて発信元のドメインを遮断したとしており、内部からの情報流出やマルウェア感染は確認されていないとのことですが、県警では不審なメールを受信した場合破棄するよう注意喚起しています。

AUS便りからの所感

KYODO

- 踏み台とされた詳しい原因は発表されていませんが、否定されている「マルウェアへの感染」以外で一般的に考えられるのは「SMTP認証アカウントに不正ログインされた」「第三者に偽装した送信元へエラーメールが送信されるよう仕向けた」あるいは「SMTP認証なしでメールの中継が可能な設定だった(オープンリレー)」等が挙げられます。
- 大量送信されたメールは英語の内容でしたが、県警を騙る巧妙な日本語のフィッシングメールが送信された場合、SPF・DKIM・DMARCによる偽メールの検知は困難となったことでしょう。
- メール送受信アカウントの厳密な管理、PCのアンチウイルスによる保護はもちろん、本来起こり得ない不審なメールの送信を食い止められるよう、サーバー自身やその前面のUTMによる送信量の制限、送信メールのスキャン・チェック、不審なログイン試行の遮断等、各種対策の実施を検討すべきでしょう。

福島県警のサーバーが不正中継　国外メール5万件

2024/11/26

福島県警察本部＝福島市杉妻町

福島県警は26日、国外から「Notice」などの件名のメール約5万件が県警のメールサーバーに送りつけられ、国内外とみられる宛先に送られたと発表した。情報流出やウイルス感染は確認されていない。県警は「再発防止策を講じた」としている。

県警によると、メールは26日午前6時～午後2時ごろ、広報活動や企業とのやりとりに使う外部向けサーバーに送られた。警察官同士がメールを送受信する内部サーバーは問題なかった。