— AUS（アルテミス・ユーザ・サポート）便り 2025/10/23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。

●大手2社で相次いでランサムウェア感染…システム障害で物流等に影響

https://internet.watch.impress.co.jp/docs/news/2054577.html
https://www.asahigroup-holdings.com/newsroom/detail/20251014-0103.html
https://www.watch.impress.co.jp/docs/news/2057222.html
https://www.askul.co.jp/snw/newsDispView/?newsId=18364

このニュースをザックリ言うと･･･

- 9月末以降、大手企業2社が相次いでランサムウェア感染によるシステム障害の被害を受け、注文の受注・商品の出荷といった物流等で影響が出ています。

- 9月29日、アサヒグループホールディングス社よりサイバー攻撃によるシステム障害の発生が発表され、傘下のアサヒビール等で商品が出荷できなくなる事態となった他、続報において個人情報が流出した可能性も確認されたとしています。

- 10月19日にはアスクル社からもランサムウェア感染が発表され、同社ECサイト「アスクル」「LOHACO」の他、同社グループ会社に物流業務委託を行っていた無印良品等もECサイトでの注文受付、実店舗での商品取り寄せ等を停止しています。

AUS便りからの所感等

- 一般にランサムウェアの侵入で最も多いとされる経路は「VPN機器からの侵入」、次いで「リモートデスクトップからの侵入」とされており、いずれも一旦侵入されると、組織内ネットワークの構成次第では内部にあるあらゆるサーバー・クライアントPCへの攻撃(いわゆるラテラル・ムーブメント)等が可能となる恐れがあります。

- これらはいずれも未修正の脆弱性を悪用されるケースが度々報告され、最新のバージョンに保つことが根本的対策としてもちろん必要ですが、一方で推測されやすいID・パスワードを悪用されるケースについても注意は欠かせません。

- アンチウイルスやUTMの単純な導入だけでランサムウェアを含めたマルウェアへの感染が100%防止できるとは限らず、UTM等を組み合わせた適切なネットワークの分割・隔離により、内部のクライアントからサーバーや他のクライアントへの不審なアクセスを遮断できるような構成も検討すべきでしょう。

- またシステム障害の発生は、韓国政府職員向けオンラインストレージがデータセンターの火災によって消失した事例(AUS便り 2025/10/09号参照)のように災害によってももたらされることもあり、システム・データともども早急な復旧のためバックアップの用意を怠らないこと、またランサムウェアによるバックアップデータの破壊の可能性も考慮し、オンラインでアクセスできない物理的に隔離された場所に保管する等が望ましいです。

Impress Watch

アサヒグループHD、サイバー攻撃に関して「流出した疑いのある情報をインターネット上で確認」と発表

山田 貞幸　2025年10月14日 08:30

アサヒグループホールディングス株式会社は、10月8日付けで、サイバー攻撃によるシステム障害について第3報を公開し、「今回の攻撃によって当社から流出した疑いのある情報をインターネット上で確認しました」と発表した。

同社では9月29日にサイバー攻撃の影響によるシステム障害について情報を公開するとともに、緊急事態対策本部を立ち上げて調査を進めている。今回確認された情報について、内容や範囲は調査中としている。また、情報漏えいの影響が確認された場合には知らせるとしている。

アスクル、ランサムウェア被害は物流システム　100名体制で対応

臼田勤哉　2025年10月23日 11:11

アスクルは22日、10月19日に発表したランサムウェア感染によるシステム障害の現状について発表した。主に物流システムにおける障害が発生し、親会社のLINEヤフーや外部セキュリティエンジニアなどを含めた対策を進めている。

この問題ではランサムウェア感染によるシステム障害が発生し、事業者向けを中心にしたEC「アスクル」や個人向けの「LOHACO」などの受注と出荷を停止している。また、グループ会社のASKUL LOGISTが受託している物流業務も停止しており、無印良品ネットストアなども停止するなど、被害が広がっている。

●9月度フィッシング報告件数は224,693件…国勢調査騙る等が確認

https://www.antiphishing.jp/report/monthly/202509.html
https://www.antiphishing.jp/news/alert/kokusei_20250922.html

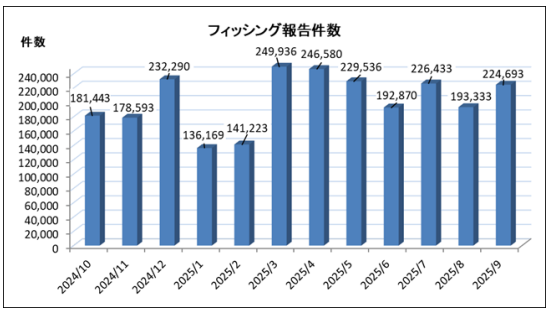
このニュースをザックリ言うと・・・

- 10月17日(日本時間)、フィッシング対策協議会より、9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。
- 9月度の報告件数は224,693件で、8月度(https://www.antiphishing.jp/report/monthly/202508.html)の193,333件から31,360件増加しています。
- 悪用されたブランド件数は111件で8月度(99件)から12件増加、割合が多かったものとしてAmazon(約15.4%)、Apple(約11.3%)が挙げられ、次いで1万件以上報告されたANA、JALと合わせて約36.0%、さらに1,000件以上報告された45ブランドまで含めると約93.3%を占めたとのことです。
- フィッシングサイトのURL件数は69,077件で8月度(76,283件)から7,206件減少、使用されるTLD(トップレベルドメイン名)の割合は10,000件以上の報告があった .com(約41.5%)、 .cn(約35.0%)、 .net(約7.3%)、 .top(約4.9%)で約88.2%を占めています。

AUS便りからの所感

- 報告件数は、5月度以降月毎に減少と増加を繰り返していますが、依然19万件超を維持しています。
- 1,000件以上報告されたブランド数は6月27ブランド→7月35ブランド→8月34ブランドを経て9月にまた急増、フィッシングサイトで使用されるTLDも .com と .cnで76.5%を占める一方、下位では多くのgTLDへ分散していたとしています。
- 9～10月実施の国勢調査において、回答依頼を騙り個人情報等を詐取しようとするフィッシングの事例が同協議会から9月22日に出されており、11月以降も事後対応を騙り様々な理由をつけてフィッシングが行われる可能性が考えられます。
- 他にも日本データ通信協会の迷惑メール相談センターには日々20件以上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等と文言が一致するか確認するとともに、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



●DNSサーバーソフト「BIND」に3件の脆弱点、セキュリティアップデートリリース

https://jprs.jp/tech/security/2025-10-23-bind9-vuln-cachepoisoning.html
https://jprs.jp/tech/security/2025-10-23-bind9-vuln-dnskey.html
https://jprs.jp/tech/security/2025-10-23-bind9-vuln-weakprng.html

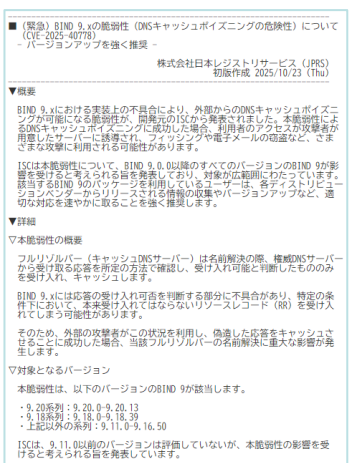
このニュースをザックリ言うと・・・

- 10月23日(日本時間)、DNSサーバー「BIND」に3件の脆弱点が発見されたとして、修正バージョン(9.20.15, 9.18.41)がリリースされました。
- 脆弱点はいずれもキャッシュDNSサーバー機能において影響を受けるとされ、悪用により、DNSキャッシュを改ざんされる(CVE-2025-40778、CVE-2025-40780)、あるいはDoS攻撃によりサーバーのパフォーマンスが低下する(CVE-2025-8677)可能性があるとされています。
- 同日にはJPRSからも、速やかにアップデートするよう注意喚起が出ています。

AUS便りからの所感

JPRS

- BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあり、近年は殆どの脆弱性がサーバープロセスのダウンやパフォーマンス低下といったDoS攻撃に繋がるものとなっていました。
- 主なLinuxディストリビューション(安定版)では、既にUbuntuについてセキュリティアップデートがリリースされており、Ubuntuの派生元のDebian、あるいはRHEL とその派生であるRocky Linux・Almalinux等についても順次リリースされるとみられます。
- 代替として他のソフトウェアあるいはCloudflare・Amazon Route 53等のクラウドサービスを使用するケースも多くなっているものの、ActiveDirectoryとの兼ね合い等でBINDを使用しているケース、メーカー製ネットワーク機器にBINDが組み込まれているケース等にも影響し得ることを鑑み、使用しているソフトウェア・機器のファームウェアについて脆弱性の有無やアップデートのリリース状況を随時確認すること、リリースされ次第適用を行うことが肝要です。



■（緊急）BIND 9.xの脆弱性（DNSキャッシュポイズニングの危険性）について
（CVE-2025-40778）
－ バージョンアップを強く推奨 －

株式会社日本レジストリサービス（JPRS）
初版作成 2025/10/23（Thu）

▼概要

BIND 9.xにおける実装上の不具合により、外部からのDNSキャッシュポイズニングが可能になる脆弱性が、開発元のISCから発表されました。本脆弱性によるDNSキャッシュポイズニングに成功した場合、利用者のアクセスが攻撃者が用意したサーバーに誘導され、フィッシングや電子メールの窃盗など、さまざまな攻撃に利用される可能性があります。

ISCは本脆弱性について、BIND 9.0.0以降のすべてのバージョンのBIND 9が影響を受けると考えられる旨を発表しており、対象が広範囲にわたっています。該当するBIND 9のパッケージを利用しているユーザーは、各ディストリビューションベンダーからリリースされる情報の収集やバージョンアップなど、適切な対応を速やかに取ることを強く推奨します。

▼詳細

▽本脆弱性の概要

フルリゾルバー（キャッシュDNSサーバー）は名前解決の際、権威DNSサーバーから受け取る応答を所定の方法で確認し、受け入れ可能と判断したもののみを受け入れ、キャッシュします。

BIND 9.xには応答の受け入れ可否を判断する部分に不具合があり、特定の条件下において、本来受け入れてはならないリソースレコード（RR）を受け入れてしまう可能性があります。

そのため、外部の攻撃者がこの状況を利用し、偽造した応答をキャッシュさせることに成功した場合、当該フルリゾルバーの名前解決に重大な影響が発生します。

▽対象となるバージョン

本脆弱性は、以下のバージョンのBIND 9が該当します。

・9.20系列：9.20.0-9.20.13
・9.18系列：9.18.0-9.18.39
・上記以外の系列：9.11.0-9.16.50

ISCは、9.11.0以前のバージョンは評価していないが、本脆弱性の影響を受けると考えられる旨を発表しています。