報道関係者各位

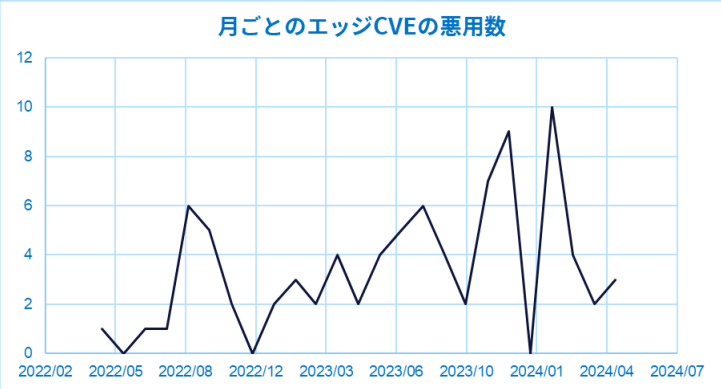
エッジサービスの大規模エクスプロイトが攻撃者の主流トレンドに
ウィズセキュア、調査レポートを発表

～ 大規模エクスプロイトがランサムウェアの主要ベクトルに ～

2024 年 6 月 18 日
ウィズセキュア株式会社

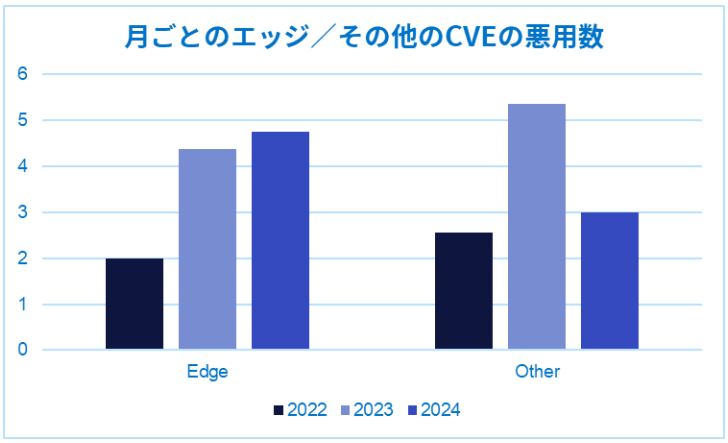
2023 年から 2024 年にかけて、私たちは多くのセキュリティ侵害を目の当たりにしてきました。2023 年に発表したレポートで当社はサイバー犯罪の専門化に関して、感染ベクトルとして大規模エクスプロイトが果たす役割が増大していることを指摘しましたが、大規模エクスプロイトの発生数と深刻度は今や爆発的に拡大しています。そうしたなか、先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (本社: フィンランド・ヘルシンキ、以下、ウィズセキュア) はエッジサービスとインフラの脆弱性に関する調査をおこない、そのレポートを発表しました。

2024 年に KEV（Known Exploited Vulnerability = 既知の悪用された脆弱性）カタログに追加されたエッジサービスおよびインフラにおける CVE（Common Vulnerabilities and Exposures = 共通脆弱性識別子）の数は、2023 年に比べて 1 ヶ月あたり 22%増加していますが、KEV に追加されたその他の CVE の数は、2023 年に比べて 1 ヶ月あたり 56%減少しています。さらに、過去 2 年間に KEV に追加されたエッジサービスおよびインフラでの CVE は、平均して他の CVE よりも深刻度が 11%高くなっています。最近発行された複数の業界レポートによると、ランサムウェアのインシデントの主要なベクトルとして、大規模エクスプロイトがボットネットを上回った可能性があります。MOVEit、CitrixBleed、Cisco XE、Fortiguard の FortiOS、Ivanti ConnectSecure、Palo Alto の PAN-OS、Juniper の Junos、ConnectWise ScreenConnect など、脆弱なソフトウェアへの大規模エクスプロイトによるセキュリティインシデントが急速に増加しています。



エッジサービスは、攻撃者にとって非常に魅力的なターゲットとなっています。これはエッジサービスがインターネットに面しており、リモートユーザーに重要なサービスを提供することを目的としているため、リモートでの攻撃をしかける脅威アクターに悪用される可能性があります。WithSecure Intelligence のシニアスレットアナリストである Stephen Robinson (スティーヴン・ロビンソン) は、こうした状況について次のように述べています。
「大規模エクスプロイトの発生に必要なものはただ 1 つ。それは、脆弱なエッジサービスです。つまり、インターネットからアクセス可能な一部のソフトウェアです。悪用されるエッジサービスの多くに共通するのは、ファイアウォール、VPN ゲートウェイ、E メールゲートウェイなどのインフラデバイスであり、一般的にロックダウンされたブラックボックス

のようなデバイスです。このようなデバイスはネットワークの安全性を高めるためのものであるはずにも関わらず、何度も脆弱性が発見され、それが攻撃者に悪用されています。」



Robinson によるリサーチでは、大規模エクスプロイトはランサムウェアを使用する脅威アクターや国家ハッカー集団にとって、新たに観測された主要な攻撃ベクトルとなっています。また、金銭的な動機を持つサイバー犯罪者にとっては、ゼロデイ脆弱性やワンデイ脆弱性を悪用するための能力や専門知識は、以前よりはるかに入手しやすい状況となっています。
「大規模エクスプロイトがメジャーな攻撃ベクトルになりつつあるのは、脆弱なエッジサービスが非常に多いため、または、大規模エクスプロイトの流行によって攻撃者と防御者が脆弱なエッジサービスをより意識するようになったためだと考えられます」と、Robinson は結論付けています。

レポート「Mass Exploitation – The Vulnerable Edge of Enterprise Security」(英語) はこちらでご覧いただけます:
https://www.withsecure.com/content/dam/with-secure/ja/resources/202406_WithSecure_Report_Mass_Exploitation_ENG.pdf

ウィズセキュア Web サイト:
https://www.withsecure.com/jp-ja/
ウィズセキュアプレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure™について

ウィズセキュアは、多くのヨーロッパ企業に選ばれるサイバーセキュリティパートナーです。世界中の IT サービスプロバイダー、MSSP、ユーザー企業から、中堅・中小企業を保護するアウトカム(成果)ベースのサイバーセキュリティソリューションにおいて大きな信頼を勝ち取っています。ウィズセキュアはヨーロッパにおけるデータ保護の規制に準拠し、プライバシー、データ主権、コンプライアンスに注力しています。
当社は 35 年以上の経験を持ち、ユーザー企業の消極的／保守的なサイバーセキュリティ対策から積極的／先進的なアプローチへのパラダイムシフトのサポートのためのポートフォリオを持っています。ウィズセキュアはパートナーとの協力的な成長へのコミットメントに基づく柔軟な商業モデルを提供し、ダイナミックなサイバーセキュリティの世界において両者の成功を保証します。
ウィズセキュアの最先端のポートフォリオの中心となるのは、AI を搭載したテクノロジー、人の専門知識、コ・セキュリティ (共同セキュリティ) サービスをシームレスに統合する Elements Cloud です。さらに、エンドポイントおよびクラウドの保護、脅威の検出と対応、エクスポージャー管理にまたがるモジュール式の機能により、中堅・中小企業ユーザーのセキュリティ対策を強固なものとします。
1988 年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご

覧ください。また、X (旧 Twitter) アカウント @WithSecure_JP https://twitter.com/WithSecure_JP でも情報の発信をおこなっています。