protiviti®
Face the Future with Confidence

さまざまなゼロデイの脆弱性を利用した Exchange Server への攻撃を Microsoft が発見

オンプレミスの Exchange Server およびすべてのハイブリッドシステムに影響があります

2021 3月4日

2021年3月2日火曜日、Microsoftはオンプレミスの Microsoft Exchange Serverのために、4つのサイクル外のセキュリティ更新プログラムをリリースしました。 これは脆弱性を狙った、これまで知られていなかった中国のスパイグループによる限定的かつ標的型の攻撃に対処するためです。この攻撃を検証し、Microsoftはただちに顧客およびセキュリティ・コミュニティへ影響があるすべてのシステムに対しパッチを共有しました。Microsoft Threat Intelligence Center（MSTIC）は、この攻撃をHafniumによるものだとし、攻撃者は企業のオンプレミスのExchange Serverにアクセスして、電子メールアカウントおよびデータを盗み出し、マルウェアをインストールしてこのアクセスを維持しようとしていると説明しました。

U.S. Cybersecurity and Infrastructure Security（CISA）partnersは、これら脆弱性への悪用を観察し、リリースされた更新内容に基づき、パッチをすぐに実装するか、あるいはMicrosoft Exchange Serverをインターネットから切断するよう連邦政府機関へ緊急指令21-02を発行しました。脅威の性質と多くの業界への潜在的な影響を考えると、企業は、影響を受けるシステムにこれらのセキュリティ更新プログラムをすぐに適用するための予防的な措置を講じる必要があります。また同時に、既存のインシデント対応で適切な危機管理ができているか評価する必要があります。

影響を受けるシステム

すべてのオンプレミスのExchange Serverとハイブリッド Exchangeシステムが影響を受けます。

注意事項：オンプレミスのActive Directory（AD）を備えたシステムでは、接続にオンプレミスのExchange Serverを使用する可能性が非常に高いです。

必要な措置

- **スキャン**—全オンプレミスのExchange Serverにおけるパッチの適用状態の記録を取得します。

- **パッチ**—セキュリティ更新をExchange Server 2010、2013、2016、および2019へ適用します。Exchange Onlineは影響を受けません。Microsoftより、当セキュリティ更新プログラムに関する解説が記載されたブログが公開され、パッチのインストールに関する質問および回答が確認できます。悪用されている脆弱性は、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、およびCVE-2021-27065です。企業は、セキュリティ更新プログラムをインストールする前に、パッチリリース記録について注意深く確認し、要件を理解することが求められます。Microsoftは、これら脆弱性に対してロールアップパッチを提供していますが、旧式ロールアップのインストールが必要になる可能性があります。さらに、SANS Instituteでは、悪用される可能性の高い脆弱性やパッチの概要を定期的に更新しています。

- **検出**—オンプレミスのExchangeおよびその他システムへの影響を評価します。Microsoftは企業が侵害の兆候や将来の攻撃を防ぐために使用できる、侵入の痕跡（IOCs）、検出ガイドそして高度な検索クエリを提供しています。Microsoft Defenderは、脆弱性に対して使用される既知の攻撃が検出可能な更新版シグニチャをリリースしました。

- **アイデンティティ／アクセス管理（IAM）プログラムとシステムの確認**—企業のアイデンティティ／アクセス管理（IAM）プログラムとシステムの強度は、攻撃者が企業環境への不正アクセスし、維持することへ重大な影響を与えます。特権アクセス管理（PAM）、アイデンティティ・

フェデレーション、セッション管理、サービスアカウント管理など、IAMプログラムの中核をなす要素はすべて、企業を守る上で重要な役割を果たします。これを機会に、企業はIAMプログラムを評価・認識し、今回のような攻撃や同様の攻撃に対する十分な防御アプローチを確保すべきです。

プロティビティの支援

プロティビティは、Microsoft 365インシデントレスポンスなどのサービスに対して、ゼロデイ脆弱性がもたらす脅威への準備と対応を支援します。プロティビティのインシデント対応チーム（IR@protiviti.com）にご連絡いただければ、技術面、危機管理面、および調査等を支援します。