本ニュースは、MORPHISEC LTD.の承諾を得たうえで、同社のブログを和訳し一部編集して掲載しています。原文は、こちらを参照ください。

マイクロソフト社の EXCHANGE サーバの脆弱性から身を守る方法

Posted by **MICHAEL GORELIK** on March 10, 2021
Find me on:
LinkedIn Twitter

Microsoft 社は、先日、攻撃者がゼロデイエクスプロイトを利用して Microsoft Exchange Server にアクセスしたことを示す攻撃について、その詳細を公開しました。この新しいエクスプロイトは、電子メールアカウントへのアクセスを可能にするものであり、被害者の環境への長期的なアクセスを容易にするために追加のマルウェアのインストールを可能にしていました。

この活動は当初、特定のグループによるものとされていましたが、現在では他の複数のグループがこの脆弱性を積極的に利用していることが明らかになっています。彼らは

通常、Covenant のようなオープンソースの正規フレームワークをコマンド＆コントロールに利用し、Mega のようなファイル共有サイトを介して被害者のデータを流出させます。

Microsoft 社は 3 月 2 日、4 つの重要な Exchange の脆弱性（CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065）を緩和するセキュリティ更新プログラムを公開しました。影響を受けるサーバのバージョンは、Microsoft Exchange Server 2013、2016、および 2019 です。

攻撃チェーン

この攻撃の初期段階では、Exchange サーバのポート 443 に対して信頼されていない接続を行う能力が必要です。攻撃者は、CVE-2021-26855 を利用して、組織の Exchange サーバへの初期アクセスを行います。この CVE は、サーバサイドリクエストフォージェリの脆弱性（SSRF）であり、攻撃者は任意の HTTP リクエストを送信し、Exchange サーバとして認証することができます。**この CVE が特に問題となるのは、この脆弱性がユーザーの操作を必要とせず、攻撃者がファイルや設定へのアクセスを必要としない点です。**攻撃者は、既知の IP または FQDN を介して、信頼されていない 443 ポートで通信します。

	CVE-2021-26855	CVE-2021-26857	CVE-2021-26858, CVE-2021-27065
CVE Description	server-side request forgery (SSRF) vulnerability in Exchange	insecure deserialization vulnerability in the Unified Messaging service	post-authentication arbitrary file write vulnerability in Exchange
Attack Vector	Network	Local	Local
Attack Complexity	Low	Low	Low
Privileges Required	None	None	None

User Interaction	None	Required	Required
Exploit code maturity	Functional	Functional	Functional
Additional Information		この脆弱性を利用すると、攻撃者は Exchange Server 上でシステムとしてコードを実行することができます。	攻撃者はこの脆弱性を利用して、サーバ上の任意のパスにファイルを書き込む可能性があります。認証が必要ですが、CVE-2021-26855 SSRF 脆弱性を悪用するか、正規の管理者の認証情報を侵害することで得られます。

CVE-2021-26857、CVE-2021-26858、および CVE-2021-27065 は、ユーザーによる操作を必要とします。そのため、攻撃者は CVE-2021-26855 を悪用するか、別の方法で Exchange を侵害する必要があります。

MORPHISEC が本攻撃から EXCHANGE サーバを守るための提案

イニシャルアクセス時のアタックサーフェスの低減

Exchange サーバをインターネットに直接公開すると、悪用される危険性が高くなります。代替案として、VPN 接続による Exchange へのアクセスを許可するか、リバースプロキシ経由で Exchange を公開することをお勧めします。これにより、侵入のリスクが大幅に軽減されます。

実行後のすべての戦術に対する徹底的な防御

真の深層防御とは、攻撃チェーンの初期段階を超えてしまった攻撃を、被害が出る前に防ぐことを意味します。最初のアクセスと特権昇格の後には、脅威主体が攻撃チェーンを続けるためにプロセスメモリの悪用を必要とするポイントが複数あります。このような重要な手口を阻止するための制御が重要になります。

Exchange のシナリオでは、Procdump と comsvcs.dll を使用して LSASS のプロセスメモリをダンプします。また、PsExec と PowerCat を使用してリモートシステムに

接続し、コマンドを送信します。最後に、PowerShell、Nishang、および Covenant フレームワークを使用して、リバースシェルの作成や新しいユー ザアカウントの作成などの変更を行います。Exchange サーバが Morphisec Keep で保護されていれば、攻撃の多くの重要なフェーズが緩和され、実行前の保護メカニズムがすべてバイパスされたとしても、侵害のリスクは大幅に減少します。

これらの脆弱性を悪用するその他の手段は、すでに侵害されたネットワークを前提としています。この場合、悪意のあるフィッシングメールを開き、ネットワーク内から Exchange サーバとの通信を開始することが考えられます。 **Morphisec は、Moving Target Defense 技術を使用して、サーバワークロードのためのゼロトラストランタイム環境を構築することで、この種の攻撃を防止します。**

迅速な可視化と封じ込め

万が一、侵害が発生した、または発生した可能性がある場合は、モルフィセックのインシデント・レスポンス・チームが支援します。当社のインシデント・レスポンス・サービスは、インシデントを封じ込め、攻撃による被害の程度を可視化します。また、今後の脅威のリスクとエクスポージャーを軽減するために、実行可能な提案を行います。

ネイティブコントロールとアップデートの活用

OS とそのネイティブコントロールを適切に設定することで、最も高度な脅威でさえも阻止することができます。また、脆弱性のあるサーバには、適切なセキュリティアップデートを適用することが重要です。

ランサムウェアのグループは、これらの脆弱性を利用してランサムウェアを展開すると予想しています。その一例として、Exchange サーバに Cobalt Strike ビーコンを導入するケースが見受けられます。

お客様や関係者の皆様にすぐにお勧めしたいのは、これらの脆弱性にパッチを適用するか、**Morphisec のような適切な代替コントロールを導入してリスクを効果的に軽減することです。**

EXCHANGE の脆弱性に関する追加情報

IOC（Indicators of Compromise）

Exchange Server チームは、パフォーマンスとメモリに関する問題に対処するため、HAFNIUM IOC のチェックを実行するスクリプトを作成しました。そのスクリプトはこちらからご覧いただけます：

https://github.com/microsoft/CSS-Exchange/tree/main/Security

インシデント・レスポンスを検討するタイミング

上記の IOC に関連する兆候が exchange サーバで発見されたり、8 文字の aspx ファイルが C:Inetpubwwwroot¥aspnet_clientsystem_web¥ ディレクトリで発見されたりした場合、インシデント・レスポンスを開始する必要があります。

Morphisec 社では、お客様ではない組織でも対応可能です。