2021年04月28日

サービス＆セキュリティ株式会社 e-Gate センター

Microsoft Exchange Server の脆弱性をついた攻撃について

1. 概要

2021 年 3 月 2 日、マイクロソフト社から Microsoft Exchange Server における緊急度の高い複数の脆弱性に関する情報が公開されました。米コンピュータ緊急事態対策チーム（US-CERT）が連日のようにアナウンスを行う異例の対応を行いその危険性が話題となりました。情報の公開から 1 か月以上経過した現在でも脆弱性を悪用するサイバー攻撃は依然として継続しており、世界中で被害が拡大しています。

今回はこの脆弱性の詳細、攻撃方法と最新の動向についてご紹介いたします。

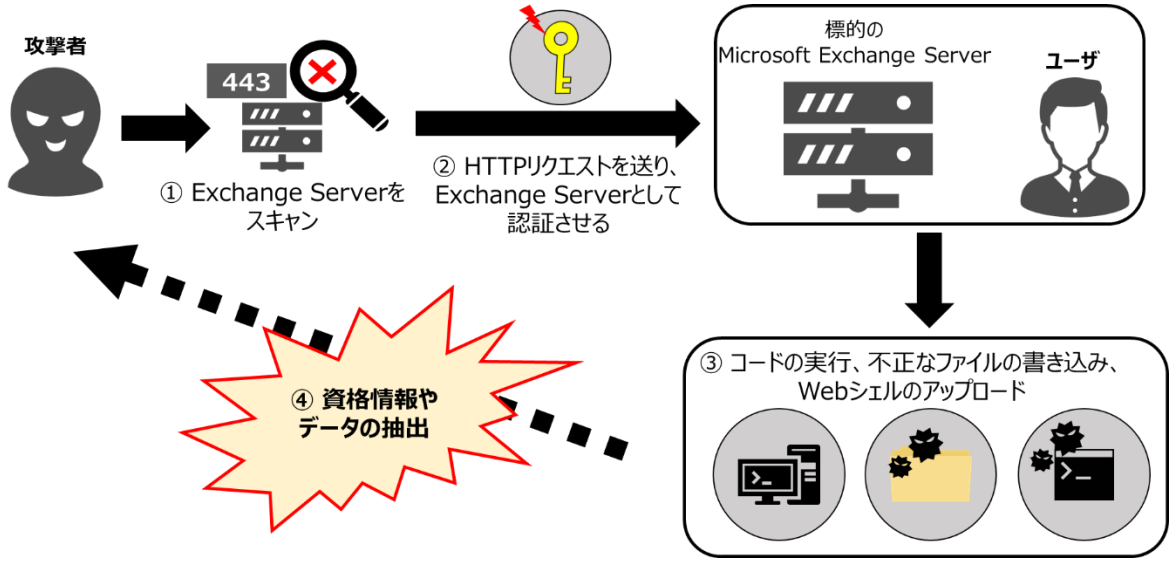
2. 脅威の詳細

Exchange Server とは、マイクロソフト社が提供する、メールサーバとグループウェアの機能を統合的に管理することができるサーバソフトウェアです。2021 年 3 月 2 日（米国時間）に Microsoft Exchange Server の複数のバージョンに影響を与える 4 つの重大なゼロデイ脆弱性が公開され、既に攻撃での悪用が確認されていることが明らかになりました。攻撃者はこの 4 つの脆弱性を悪用し、インターネットに公開されている Microsoft Exchange Server へ不正アクセスしてサーバを悪用することができます。なお、4 つのゼロデイ脆弱性は全てパッチがリリースされています。

【表 1】4 つの重大な脆弱性

共通脆弱性識別子 (CVE)	説明
CVE-2021-26855	サーバサイドリクエスト偽造（SSRF:Server-Side Request Forgery）の脆弱性。 任意の HTTP リクエストを送信して攻撃者が自身を Exchange Server として認証させることが可能。この脆弱性は「ProxyLogon」と呼称されている。
CVE-2021-26857	Unified Messaging サービスにおける安全でないデシリアライズの脆弱性。 Microsoft Exchange Server において高度な権限（SYSTEM）を持つコードを実行することが可能。この脆弱性を用いるには管理者権限か、別の脆弱性を組み合わせる必要がある。
CVE-2021-26858	Microsoft Exchange Server における認証後に任意ファイルの書き込みができる脆弱性。 CVE-2021-26855 と組み合わせて攻撃者が自身を Exchange Server として一度認証させることで、サーバ上の任意の場所にファイルを配置することができる。
CVE-2021-27065	Microsoft Exchange Server における認証後に任意ファイルの書き込みができる脆弱性。 CVE-2021-26855 と組み合わせて攻撃者が自身を Exchange Server として一度認証させることで、サーバ上の任意の場所にファイルを配置することができる。

今回の 4 つの脆弱性を悪用した攻撃方法の一例については図 1 のとおりとなります。



【図 1】Microsoft Exchange Server の脆弱性をついた攻撃方法の一例

① 攻撃者は外部から443ポートにてアクセス可能なオンプレミスの Microsoft Exchange Server を探し特定します。
② 任意の HTTP リクエストを送信することで攻撃者が自身を Exchange Server として認証させて、管理者に成りすましします。（CVE-2021-26855）
③ SYSTEM 権限でコードを実行することが可能な脆弱性（CVE-2021-26857）、攻撃者が自身を Exchange Server として認証させた後に任意ファイルの書き込みが可能となる脆弱性（CVE-2021-26858、CVE-2021-27065）を悪用することで、Web シェルのアップロードや任意のコマンドを実行することができます。
④ 攻撃者は資格情報やデータを抜き取り漏出させます。

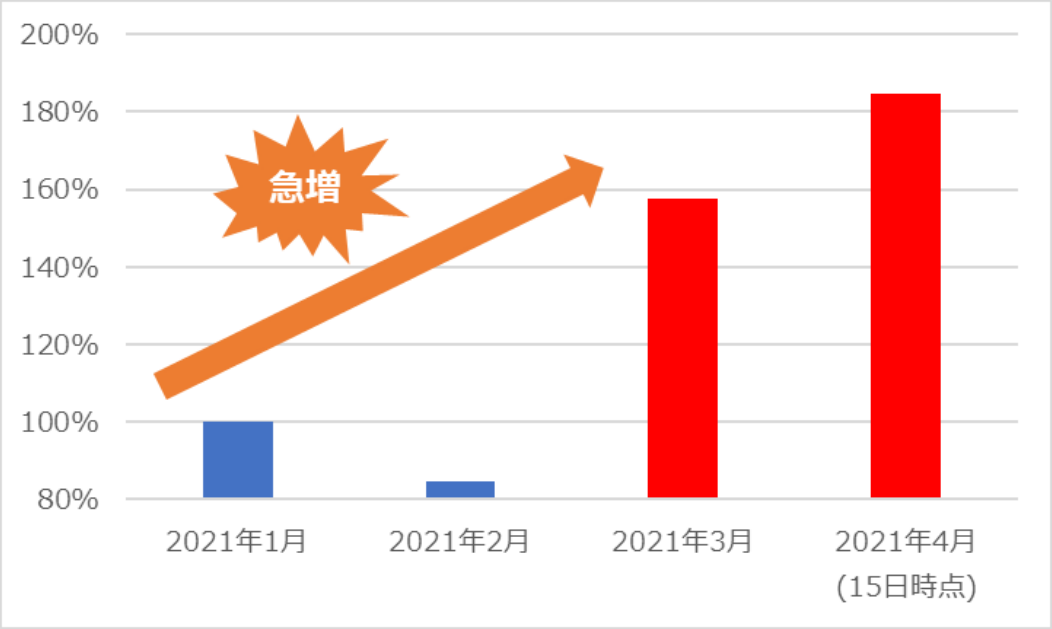
このように Microsoft Exchange Server の脆弱性を悪用されることにより、情報漏出などの被害が発生する可能性があります。その他にもランサムウェアを使用する事例も報告されています。また、設置された Web シェルにより任意コマンドの実行やファイル更新、削除、参照が行われるだけでなく、Web シェルは後続の攻撃者の侵入経路となる危険性もあります。

3. 最新動向

Microsoft Security Response Center は 3 月 23 日（米国時間）、公式の Twitter アカウントにおいて、92%の Microsoft Exchange Server に「パッチを適用した」または「緩和策を適用した」と公表しました。インシデントは継続中でありながら、脆弱性情報の公開以降パッチの適用が相次いで行われたことで大きな進歩があったことを報告しています。しかし、Microsoft Exchange Server の脆弱性を対象としたランサムウェア攻撃の増加が確認されるなど、本脆弱性を悪用する攻撃は依然として継続しており、長期化する恐れもあり、注意が必要です。

4. e-Gate センターにおける攻撃検知の推移

e-Gate センターでは Microsoft Exchange Server の脆弱性をついた攻撃の増加を観測しております。今年の 2 月と比較して、3 月は大幅に検知数が増加しています。また、4 月以降もその検知数に増加の兆しがあることから本脆弱性を悪用した攻撃が今後長期に渡り発生することも推測されます。実際の推移観測結果が図 2 となります。



【図 2】e-Gate センターにおける Microsoft Exchange Server の脆弱性をついた攻撃イベント数の推移
（2021 年 1 月を 100%として算出）

5. 攻撃対策

・最新のアップデートの適用

脆弱性を修正する更新プログラムを Microsoft が公開しています。対象バージョンのシステムを使用している場合、インストールすることが推奨されます。

・セキュリティ機器による攻撃通信の監視

Microsoft Exchange Server のポート 443 への不正アクセスを Firewall や IPS（侵入防御システム）で拒否することで、攻撃の初期段階を阻止することができます。

前述のとおり Microsoft Exchange Server への攻撃は今後長く継続すると推測され、攻撃の被害にあう可能性があります。Firewall や IPS、UTM といったセキュリティ機器により攻撃通信を検知、防御することで、被害を最小限に抑えることができます。何よりも、いち早く攻撃に気付けるような仕組みと監視体制を徹底しておくことが有効な対策となります。

6. e-Gate の監視サービスについて

攻撃対策にある通り、セキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。

"e-Gate"の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。"e-Gate"の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

7. 参考情報

・Microsoft

Released: March 2021 Exchange Server Security Updates

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

・米コンピュータ緊急事態対策チーム（US-CERT）

Citrix Releases Security Updates for Hypervisor

https://us-cert.cisa.gov/ncas/current-activity/2021/03/31/citrix-releases-security-updates-hypervisor

・Microsoft Security Response Center 公式 Twitter アカウント（@msftsecresponse）

https://twitter.com/msftsecresponse/status/1374075310195412992

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
　リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp