2021 年 3 月吉日

パートナー様各位

日本マイクロソフト株式会社

Exchange Server のゼロデイ脆弱性に対する
定例外のセキュリティ更新プログラムの公開について

拝啓

貴社ますますご隆盛のこととお慶び申し上げます。平素は格別のお引き立てを賜り、厚くお礼申し上げます。

昨日、マイクロソフトは、国家の関与が疑われるグループによって悪用される可能性のある、オンプレミスの Microsoft Exchange Server のゼロデイの脆弱性に対するセキュリティ更新プログラムをリリースしました。本脆弱性は Exchange Server の複数のバージョンに影響があり、Exchange Server 2010 (多層防御の観点)、2013、2016、2019 が対象となります。Exchange Online は影響を受けません。弊社のアカウント マネージャーとテクニカル サポート チームは、パートナー様のテクニカル チームと連携して、この問題に対処するための支援を行います。 パートナー様には、この状況をご認識いただき、早急な改善策を講じていただきたいと考えています。

オンプレミスの Exchange Server への適用については、インターネットからアクセス可能なサーバー（例：Outlook on the Web/OWA や ECP を公開しているサーバー）を最優先とし、Exchange インフラストラクチャの評価と脆弱性のあるサーバーへのセキュリティ更新プログラムの適用を直ちに行ってください。 これらの脆弱性にセキュリティ更新プログラムを適用するには、最新の Exchange Server の累積更新プログラムを適用してから、本日公開した各 Exchange Server のセキュリティ更新プログラムをインストールする必要があります。

Exchange Server Health Checker スクリプトは、GitHub からダウンロードできます（最新のリリースを使用してください）。このスクリプトを実行すると、オンプレミスの Exchange Server の更新が遅れているかどうかがわかります（このスクリプトは Exchange Server 2010 をサポートしていない点をご留意ください）。また、セキュリティチームが脆弱性が悪用されているかどうかを評価する際には、ここで共有した「セキュリティ侵害インジケーター」を利用することをお勧めします。

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

私たちは、弊社のアカウントチームとサポートチームを通じてこの問題を解決するためにパートナー様と協力することをお約束します。

以上

Microsoft Digital Trust

関連情報

推奨するアクション

- マイクロソフトは、本脆弱性に対応するために本日公開したセキュリティ更新プログラムを、優先度を高くして展開することをお勧めします。
- リスクが高まっている、インターネットに接続された Exchange Server への適用を優先してください。
- 今回のセキュリティ更新プログラムを適用するには、サポートされている Update Rollup (UR) や Cumulative Update (CU) が必要となります。サポートされている Update Rollup (UR) や Cumulative Update (CU) を適用していない場合には、先にこれらの更新プログラムを適用する作業が必要です。
- 下記の外部向け情報や内部向け情報にて、脆弱性に関する詳細や推奨するアクション、セキュリティ更新プログラムの入手先をご確認ください

公開情報

- JPSRT Blog: https://msrc-blog.microsoft.com/2021/03/02/20210303_exchangeoob/ (日本語)
- Exchange Team Blog: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901 (英語)
- MSRC blog: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server (英語)
- MSTIC blog: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (英語)
- Microsoft On The Issues (MOTI) blog: https://blogs.microsoft.com/on-the-issues/?p=64505 (英語)

脆弱性情報の詳細

March 2, 2021 Security Update Release - Release Notes - Security Update Guide - Microsoft
CVE-2021-26412
CVE-2021-26854
CVE-2021-26855
CVE-2021-26857
CVE-2021-26858
CVE-2021-27065
CVE-2021-27078

セキュリティ更新プログラムの適用についてサポートが必要なパートナー様は、以下のお問い合わせ先にご連絡ください。
(なお当該件に関するご支援は無償で提供いたします。Exchange Server セキュリティ更新プログラムの適用についてのお問い合わせであることを、窓口へお伝えください。)

1. プロフェッショナル サポート、又は Advanced Support for Partners/Premier Support for Partners のご契約をお持ちのパートナー様

プロフェッショナルサポート

プロフェッショナル サポートをご利用になる皆様へ
https://www.microsoft.com/ja-jp/services/professional.aspx

プロフェッショナル サポートご利用の流れ
https://www.microsoft.com/ja-jp/services/professional-guide.aspx

プロフェッショナル サポートをご利用の皆様へ
https://www.microsoft.com/ja-jp/services/professional-supportqa.aspx

Advanced Support for Partners/Premier Support for Partners
担当カスタマーサクセスアカウントマネージャへご連絡ください

2．プロフェッショナルサポート、Advanced Support for Partners/Premier Support for Partners のご契約をお持ちでないパートナー様

お問い合わせ先
TEL：0120-17-0196 FAX：0120-74-0196
営業時間：9:00 ～ 17:30（土日祝日、弊社指定休業日を除く）

追加のサポートが必要な場合は弊社のビジネスディベロップメントマネージャーにお知らせください。