Cisco Meraki MX シリーズおよび Z シリーズのクライアント証明書認証を使用した AnyConnect VPN におけるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-meraki-mx-vpn-dos-sM5GCfm7
初公開日 : 2025-06-18 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID :

CVE-2025-20271

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Meraki MX シリーズおよび Cisco Meraki Z シリーズ テレワーカー ゲートウェイ デバイスの Cisco AnyConnect VPN サーバーにおける脆弱性により、認証されていないリモートの攻撃者が該当デバイス上の Cisco AnyConnect サービスにサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、SSL VPN セッションが確立される際の変数の初期化エラーに起因します。攻撃者は、該当デバイスに巧妙に細工された一連の HTTPS 要求を送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は Cisco AnyConnect VPN サーバーを再起動させ、その結果、確立されたすべての SSL VPN セッションが失敗し、リモートユーザーは新しい VPN 接続を開始し、再認証しなければならない可能性があります。攻撃が続けば、新しい SSL VPN 接続の確立が妨げられ、事実上、すべての正当なユーザーが Cisco AnyConnect VPN サービスを利用できなくなる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

該当製品

脆弱性のある製品

この脆弱性は、Cisco Meraki MX ファームウェアの脆弱性が存在するリリースを実行し、クライアント証明書認証を有効にした Cisco AnyConnect VPN を使用している次の Cisco Meraki 製品に影響を与えます。

• MX64 • MX64W • MX65 • MX65W • MX67 • MX67C • MX67W	• MX68 • MX68CW • MX68W • MX75 • MX84 • MX85 • MX95	• MX100 • MX105 • MX250 • MX400 • MX450 • MX600 • vMX	• Z3 • Z3C • Z4 • Z4C

注：Cisco AnyConnect VPN は、Cisco Meraki MX ファームウェアリリース 16.2 以降が稼働する Cisco Meraki MX シリーズおよび Cisco Meraki Z シリーズ デバイスでサポートされます。ただし、Cisco Meraki MX ファームウェアリリース 17.6 以降が稼働している場合にのみ Cisco AnyConnect VPN をサポートする Cisco Meraki MX64 および MX65 は除きます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

デバイス設定の確認

Cisco Meraki MX シリーズまたは Cisco Meraki Z シリーズ デバイスで、クライアント証明書認証を使用した Cisco AnyConnect VPN が有効になっているかどうかを確認するには、次の手順を実行します。

1. [ダッシュボード（Dashboard）] にログインします。
2. 2 番目の手順は、プラットフォームとライセンスレベルによって若干異なります。
    - Cisco Meraki MX デバイスの場合、統合されたビューで [セキュリティとSD-WAN（Security & SD-WAN）] > [設定（Configure）] > [クライアントVPN（Client VPN）] を選択します。
    - Cisco Meraki Z シリーズ デバイスの場合、統合されたビューで、[テレワーカーゲートウェイ（Teleworker gateway）] > [設定（Configure）] > [クライアントVPN（Client VPN）] を選択します。
3. [AnyConnect設定（AnyConnect Settings）] タブを選択します。
    - [有効（Enabled）] オプションボタンが選択されている場合、デバイスは Cisco AnyConnect VPN をサポートするように設定されており、デバイスはこのアドバイザリで説明されている脆弱性の影響を受ける可能性があります。ステップ 4 に進みます。
    - [Cisco AnyConnect設定（Cisco AnyConnect Settings）] タブが表示されていない場

合、または [無効（Disabled）] オプションボタンが選択されている場合、デバイスはこの脆弱性の影響を受けません。

4. [認証とポリシー（Authentication & policy）] セクションまで下にスクロールします。
    - [証明書認証（Certificate authentication）] が [有効（Enabled）] に設定されている場合、クライアント証明書認証が有効になり、デバイスはこの脆弱性の影響を受けます。
    - [無効（Disabled）] に設定されている場合、デバイスはこの脆弱性の影響を受けません。

追加情報

Cisco Meraki MX シリーズおよび Cisco Meraki Z シリーズ デバイスは、リモート ネットワーク アクセス用に次の 2 つの VPN サービスをサポートしています。

- レイヤー 2 トンネリングプロトコル（L2TP）または IPsec トンネリングプロトコルを使用するクライアント VPN
- TLS および Datagram TLS（DTLS）プロトコルを使用し、一般に SSL VPN と呼ばれる Cisco AnyConnect VPN

Cisco Meraki MX シリーズおよび Cisco Meraki Z シリーズ デバイスの両方で、クライアント VPN（L2TP/IPsec）および Cisco AnyConnect VPN（SSL）サービスを同時に有効にできます。

注：この脆弱性は、SSL VPN セッションの確立中に存在するため、Cisco AnyConnect VPN が設定されているデバイスのみに影響します。クライアント VPN（L2TP/IPsec）のみを通じてリモート ネットワーク アクセスを提供するように設定されているデバイスは、この脆弱性の影響を受けません。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Threat Defense（FTD）ソフトウェア
- IOS ソフトウェア
- IOS XE ソフトウェア
- Meraki Z1

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

Cisco Meraki では、このアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。Cisco Meraki では、お客様が修正済みのリリースにアップグレードすることを推奨しています。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアリリースとフィーチャセットに対してのみとなります。お客様は、このようなソフトウェアアップグレードをインストール、ダウンロード、アクセス、またはその他の方法で使用することにより、シスコ エンド ユーザー ライセンス契約および該当する製品固有の条件に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、Cisco Meraki から直接、あるいは Cisco Meraki 認定リセラーやパートナーから、ソフトウェアの有効なライセンスを取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

お客様は、[シスコセキュリティアドバイザリ（Cisco Security Advisories）] ページで入手できる Cisco Meraki 製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認することをお勧めします。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。Cisco Meraki は、ファームウェアの更新にファームウェアのベストプラクティスを利用することを推奨しています。情報が明確でない場合は、Cisco Meraki サポートに問い合わせることをお勧めします。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。Cisco Meraki は、必要に応じてこのアドバイザリを更新します。

次の表の左側の列は、Cisco Meraki ファームウェアリリースを示しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Meraki MX ファームウェアリリース	First Fixed Release（修正された最初のリリース）
16.2 より前	影響なし。
16.2	修正済みリリースに移行。

Cisco Meraki MX ファームウェアリリース	First Fixed Release（修正された最初のリリース）
17	修正済みリリースに移行。
18.1xx	18.107.13
18.2xx	18.211.6
19.1	19.1.8

注：

- Cisco Meraki MX64 および MX65 は、Cisco Meraki MX ファームウェアリリース 17.6 以降を実行している場合にのみ影響を受けます。
- Cisco Meraki MX400 および MX600 は、ファームウェアリリース 16.16.9 以前のみをサポートします。これらのモデルはサポート終了プロセスに入っており、この脆弱性に対する修正は提供されません。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

この脆弱性は Cisco Meraki サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2025 年 6 月 18 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり

する権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。