Cisco Meraki MXおよびZシリーズのAnyConnect VPNにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-meraki-mx-vpn-dos-vNRpDvfb
初公開日 : 2025-04-02 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCwk81017

CVE-2025-20212

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およびCisco Meraki Zシリーズデバイスの Cisco AnyConnect VPNサーバにおける脆弱性により、認証されたリモート攻撃者が、該当デバイスのCisco AnyConnectサービスでサービス妨害(DoS)状態を引き起こす可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスで有効なVPNユーザクレデンシャルを持っている必要があります。

この脆弱性は、SSL VPNセッションの確立時に変数が初期化されないことに起因しています。攻撃者は、該当デバイスとのSSL VPNセッションを確立する際に、巧妙に細工された属性を提供することにより、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、攻撃者がCisco AnyConnect VPNサーバを再起動できるようになり、確立されたSSL VPNセッションが失敗し、リモートユーザが新しいVPN接続を開始して再認証を実行する必要が生じる可能性があります。攻撃が持続的であれば、新しい SSL VPN 接続の確立が妨げられる可能性があります。

注：攻撃トラフィックが停止すると、Cisco AnyConnect VPNサーバは手動による介入なしで回復します。

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-vNRpDvfb

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、Cisco AnyConnect VPN が有効になっている次の 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以降を実行しているCisco Meraki MXおよびCisco Meraki Zシリーズデバイスでサポートされています。ただし、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Cisco AnyConnect VPNをサポートするCisco Meraki MX64およびMX65を除きます。

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。

Cisco AnyConnect VPNが有効になっているかどうかの確認

Cisco Meraki MXまたはCisco Meraki Zシリーズデバイスで Cisco AnyConnect VPNが有効になっているかどうかを確認するには、次の手順に従います。

1. ダッシュボードにログインします。
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少し異なります。
    - Cisco Meraki MXデバイスの場合、統合ビューでSecurity & SD-WAN > Configure > Client VPNの順に選択します。
    - Cisco Meraki Zシリーズデバイスの場合、統合ビューでTeleworker Gateway > Configure > Client VPNの順に選択します。
3. AnyConnect Settingsタブを選択します。

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います。

Cisco AnyConnect Settingsタブが表示されない場合、またはDisabledオプションボタンが選択された場合、デバイスは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ません。

追加情報

Cisco Meraki MX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
- Cisco AnyConnect VPN:TLSおよびDatagram TLS(DTLS)プロトコルを使用し、一般にSSL VPNと呼ばれます。

Cisco Meraki MX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)サービスと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セッションの確立時に発生するため、影響を受けるのはCisco AnyConnect VPNが設定されたデバイスだけです。クライアントVPN(L2TP/IPsec)のみを介し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、修正済みリリースへのアップグレードを推奨しています。

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。

お客様は定期的にCisco Security Advisoriesページで入手できるCisco Meraki製品のアドバイザリを参照して、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してください。

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では、ファームウェアのアップデート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。不明な点については、Cisco Merakiサポートまでお問い合わせください。

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。
17	修正済みリリースに移行。
18.1	18.107.12
18.2	18.211.4
19.1	19.1.4

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16.2以前のみをサポートしています。これらのモデルはサポート終了プロセスに入っており、この脆弱性の修正は提供されません。

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された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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

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

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4月2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。