# Cisco Meraki MXおよびZシリーズテレワーカーゲートウェイのAnyConnect VPNセッションのテイクオーバーおよびサービス妨害(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID :

CVE-2024-20509

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シリーズテレワーカーゲートウェイデバイスの Cisco AnyConnect VPNサーバの脆弱性により、認証されていないリモートの攻撃者がAnyConnect VPNセッションをハイジャックしたり、該当デバイスのAnyConnect VPNサービスの個々のユーザにサービス妨害(DoS)状態を引き起こしたりする可能性があります。

この脆弱性は、VPN認証プロセスで使用されるハンドラのエントロピーが弱いこと、および同じプロセス内に競合状態が存在することが原因で発生します。攻撃者は、認証ハンドラを正しく推測し、巧妙に細工されたHTTPS要求を該当デバイスに送信することで、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、攻撃者はターゲットユーザからAnyConnect VPNセッションを引き継いだり、ターゲットユーザが該当デバイスとのAnyConnect VPNセッションを確立することを阻止したりできる可能性があります。

Cisco Meraki では、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-by-QWUkqV7X

## 該当製品

### 脆弱性のある製品

公開時点で、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ていて、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した。

| | | | |
|---|---|---|---|
| • MX64<br>• MX64W<br>• MX65<br>• MX65W<br>• MX67<br>• MX67C<br>• MX67W | • MX68<br>• MX68CW<br>• MX68W<br>• MX75<br>• MX84<br>• MX85<br>• MX95 | • MX100<br>• MX105<br>• MX250<br>• MX400<br>• MX450<br>• MX600<br>• vMX | • Z3<br>• Z3C<br>• Z4<br>• 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シリーズテレワーカーゲートウェイ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。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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 Meraki MX デバイスで Cisco AnyConnect VPN が有効になっているかどうかの確認

Cisco Meraki MX 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、次の手順を実行します。

1. [Dashboard] にログインします。
2. 統合ビューで、[Dashboard] > [Configure] > [Client VPN] を選択します。
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る場合、デバイスはこの脆弱性の影響を受けません。

## Cisco Meraki Zシリーズテレワーカーゲートウェイデバイスで Cisco AnyConnect VPNが有効になっているかどうかの確認

Cisco Meraki MX 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、次の手順を実行します。

1. [Dashboard] にログインします。
2. 統合ビューで、[Teleworker gateway] > [Configure] > [Client VPN] を選択します。
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る場合、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記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Meraki Z1
- 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

## 回避策

この脆弱性に対処する回避策はありません。Cisco Meraki では、管理者がデバイスを修正済みのソフトウェアリリースにアップグレードすることを推奨しています。

ただし、Cisco AnyConnect VPNを無効にすると、このアドバイザリで説明されている脆弱性に対する攻撃ベクトルが排除されます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ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アップグレード ソリューション一式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。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーに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。

左の列にはCisco Merakiソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された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リリースが示されています。

| 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 以降 | 修正済みリリースに移行。 |
| 17.0 以降 | 修正済みリリースに移行。 |
| 18.0 以降 | 18.211.3 |

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。

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およびCisco Meraki Incident Response Team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は確認しておりません。

## 出典

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKeane O'Kelley氏による社内セキュリティテストで発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X

## 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 | 2024年10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。