Cisco Meraki MX および Z シリーズ テレワーカー ゲートウェイ 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-QTRHzG2
初公開日 : 2024-10-02 16:00
最終更新日 : 2025-06-02 14:22
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID :

CVE-2024-20498
CVE-2024-20500
CVE-2024-20499
CVE-2024-20502
CVE-2024-20513
CVE-2024-20501

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 サーバーにおける複数の脆弱性により、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 AnyConnect VPN 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。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

Cisco Meraki はこれらの脆弱性に対処するソフトウェアアップデートを提供しています。これら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-QTRHzG2

該当製品

脆弱性のある製品

これらの脆弱性は、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。

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 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. [ダッシュボード（Dashboard）] にログインします。
2. 統合ビューで [セキュリティアプライアンス（Security Appliance）] > [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います。

[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、デバイスはこのアドバイザリで説明されている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. [ダッシュボード（Dashboard）] にログインします。
2. 統合ビューで [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います。

[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、デバイスはこのアドバイザリで説明されている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 テレワーカー ゲートウェイ 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
- Transport Layer Security（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 シリーズと Cisco Meraki Z シリーズ テレワーカー ゲートウェイ 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：これらの脆弱性は、TLS および DTLS パケットの処理に存在するため、Cisco AnyConnect VPN が設定されているデバイスにのみ影響します。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、これら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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性を工クスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20498、CVE-2024-20499、および CVE-2024-20501：Cisco Meraki MX および Z シリーズ テレワーカー ゲートウェイ AnyConnect VPN DoS の脆弱性

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 サーバーにおける複数の脆弱性により、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 AnyConnect サービスに DoS 状態を引き起こす可能性があります。

これらの脆弱性は、SSL VPN セッションの確立中にクライアントが提供するパラメータの検証が不十分であることに起因します。攻撃者は、巧妙に細工された HTTPS リクエストを該当デバイスの VPN サーバーに送信することで、これらの脆弱性をエクスプロイト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 SSL VPN 接続が失敗し、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 サーバーは、手動による介入を必要とせずに正常に回復します。

Cisco Meraki はこれらの脆弱性に対処するソフトウェアアップデートを提供しています。これらの脆弱性に対処する回避策はありません。

CVE ID：CVE-2024-20498、CVE-2024-20499、CVE-2024-20501
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.6
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2024-20500：Cisco Meraki MX および Z シリーズ テレワーカー ゲートウェイ AnyConnect VPN DoS の脆弱性

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 AnyConnect サービスに DoS 状態を引き起こす可能性があります。

この脆弱性は、TLS/SSL セッションを確立する際の不十分なリソース管理に起因します。攻撃者は、巧妙に細工された一連の TLS/SSL メッセージを該当デバイスの VPN サーバーに送信するこ

とで、この脆弱性をエクスプロイト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 サーバーに新しい接続の受け入れを停止させ、新しい SSL VPN 接続を確立できないようにする可能性があります。既存の SSL VPN セッションは影響を受けません。

注：攻撃トラフィックが停止すると、Cisco AnyConnect VPN サーバーは、手動による介入を必要とせずに正常に回復します。

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。

CVE ID：CVE-2024-20500
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2024-20502：Cisco Meraki MX および Z シリーズ テレワーカー ゲートウェイ AnyConnect VPN DoS の脆弱性

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に 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 セッションを確立する際の不十分なリソース管理に起因します。攻撃者は、巧妙に細工された一連の HTTPS リクエストを該当デバイスの VPN サーバーに送信することで、この脆弱性をエクスプロイト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 サーバーに新しい接続の受け入れを停止させ、新しい SSL VPN 接続を確立できないようにする可能性があります。既存の SSL VPN セッションは影響を受けません。

注：攻撃トラフィックが停止すると、Cisco AnyConnect VPN サーバーは、手動による介入を必要とせずに正常に回復します。

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。

CVE ID：CVE-2024-20502
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2024-20513：Cisco Meraki MX および Z シリーズ テレワーカー ゲートウェイ AnyConnect VPN を標的とした DoS の脆弱性

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 AnyConnect サービスの標的ユーザーに 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 セッションの確立中に使用されるハンドラのエントロピーが不十分であることに起因します。認証されていない攻撃者は、有効なセッションハンドラにブルートフォース攻撃を仕掛けることで、この脆弱性をエクスプロイトする可能性があります。認証された攻撃者は、該当デバイスの AnyConnect VPN サービスに接続して有効なセッションハンドラを取得し、そのハンドラに基づいてさらに有効なセッションハンドラを予測することで、この脆弱性をエクスプロイトする可能性があります。次に、攻撃者は、ブルートフォース攻撃を仕掛けたセッションハンドラまたは予測したセッションハンドラを使用して、細工された HTTPS リクエストをデバイスの AnyConnect VPN サーバーに送信します。エクスプロイトに成功すると、攻撃者は標的の SSL VPN セッションを終了し、その結果、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。

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。

CVE ID：CVE-2024-20513
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

回避策

これら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、これらの脆弱性の緩和策として、Cisco AnyConnect VPN を無効にすると、このアドバイザリに記載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

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。

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、およびこれら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	18.211.2

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。

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 Product Security Incident Response Team（PSIRT）および Cisco Meraki Incident Response Team は、本アドバイザリに記載されている脆弱性のエクスプロイト事例は確認していません。

出典

これらの脆弱性は、内部セキュリティテストの実施中に、Cisco Advanced Security Initiatives Group（ASIG）の Keane O'Kelley 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-QTRHzG2

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	修正済みリリースの入手状況を更新。	修正済みリリース	Final	2025 年 6 月 2 日
1.0	初回公開リリース	—	Final	2024 年 10 月 2 日

利用規約

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。