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におけるサービス妨害(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-meraki-mx-vpn-dos-QTRHzG2
初公開日 : 2024-10-02 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-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リリースしました。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. [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。

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シリーズの両方のテレワーカーゲートウェイデバイスで、クライアントVPN(L2TP/IPsec)とCisco AnyConnect VPN(SSL)の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パケットとDTLSパケットの処理に存在するため、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エ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のAnyConnect VPNにおけるDoS脆弱性

Cisco Meraki MXデバイスおよび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指定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、該当デバイスのVPNサーバに巧妙に細工された HTTPS要求を送信することにより、これら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サーバを再起動させ、確立されたSSL VPN接続に障害を発生させ、リモートユーザに新しいVPN接続を開始させて再認証を強制す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リリースしました。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のAnyConnect VPNにおけるDoS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リソース管理が不十分であることに起因します。攻撃者は、一連の巧妙に細工されたTLS/SSLメッセージを該当デバイスのVPNサーバに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。不正利用に成功すると、攻撃者はCisco AnyConnect VPNサーバに新しい接続の受け入れを停止させ、新しいSSL VPN接続の確立を阻止する可能性があります。既存のSSL VPNセッションには影響しません。

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のAnyConnect VPNにおけるDoS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リソース管理が不十分であることに起因します。攻撃者は、該当デバイスのVPNサーバに一連の巧妙に細工された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。不正利用に成功すると、攻撃者はCisco AnyConnect VPNサーバに新しい接続の受け入れを停止させ、新しいSSL VPN接続の確立を阻止する可能性があります。既存のSSL VPNセッションには影響しません。

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のAnyConnect VPNで標的となるDoS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、該当デバイスでAnyConnectサービスのターゲットユーザに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セッションの確立時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をブルートフォーシングすることで、この脆弱性を不正利用する可能性があります。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、この脆弱性を不正利用する可能性があります。攻撃者は、ブルート強制または予測セッションハンドラを使用して、巧妙に細工されたHTTPS要求をデバイスのAnyConnect VPNサーバに送信します。エクスプロイトに成功すると、攻撃者はターゲットのSSL VPNセッションを終了し、リモートユーザに新しいVPN接続を開始させ、再認証を強制す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。

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、これらの脆弱性を緩和するために、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、テスト環境に導入して効果を発揮することが実証されていますが、お客様の環境や使用条件における適用性と有効性を確認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提供しています。

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、[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。

次の表では、左の列にCisco Merakiファームウェアリリースを示します。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 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	18.211.2

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。

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 Product Security Incident Response Team(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

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKeane O'Kelley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-QTRHzG2

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	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。