ワイヤレスコントローラ用Cisco IOS XEソフトウェアのCWA事前認証ACLバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-c9800-cwa-acl-nPSbHSnA
CVE-2024-20510
初公開日 : 2024-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 4.7
回避策 : Yes
Cisco バグ ID : CSCwh81471

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

ワイヤレスコントローラ用Cisco IOS XEソフトウェアの中央Web認証(CWA)機能における脆弱性により、認証されていない隣接する攻撃者が事前認証アクセスコントロールリスト(ACL)をバイパスし、ユーザ認証の前にネットワークリソースへのアクセスを許可する可能性があります。

この脆弱性は、認証、許可、アカウンティング(AAA)サーバから受信した事前認証ACLをアクティブ化する際の論理エラーが原因で発生します。攻撃者は、CWA用に設定されたワイヤレスネットワークに接続し、ユーザ認証の前に設定されたACLによって拒否される必要がある該当デバイスを介してトラフィックを送信することで、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、ユーザ認証が完了する前に、該当デバイスで設定されているACL保護を攻撃者がバイパスし、デバイスが保護している可能性のある信頼できるネットワークにアクセスできるように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。本脆弱性に対処する回避策がいくつかあります。

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-c9800-cwa-acl-nPSbHSnA

このアドバイザリは、Cisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2024年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2024 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、Cisco IOS XEソフトウェアの脆弱性のあるリリースを実行し、CWAを有効にしている次のシスコ製品に影響を与えました。

- クラウド向け Catalyst 9800-CL ワイヤレスコントローラ
- Catalyst 9300、9400、9500 シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Catalyst 9800 シリーズ ワイヤレス コントローラ
- Catalyst アクセスポイントの組み込みワイヤレスコントローラ

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。

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。

- IOS ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- ワイヤレス LAN コントローラ（WLC）AireOS ソフトウェア

詳細

この脆弱性が不正利用されると、攻撃者は該当デバイスに適用されるACLによって提供される保護をバイパスできる可能性があります。この脆弱性の全体的な影響は、ACLで保護する必要がある資産の重要性に依存するため、組織によって異なります。お客様は、この脆弱性の不正利用がネットワークに与える影響を評価し、お客様独自の脆弱性処理および修復プロセスに従って作業を進める必要があります。

回避策

この脆弱性に対処する回避策があります。必要に応じて、IPv4 ACLまたはIPv6 ACLを追加します。

IPv6 ACLの追加

ワイヤレスコントローラに設定されているリダイレクションACLがIPv4 ACLである場合、すべてのトラフィックを拒否する新しいIPv6 ACLを作成し、CWA認証フェーズで適用する必要があります。これを行うには、次の手順を実行します。

まず、ワイヤレスコントローラで次の操作を実行します。

1. Web管理インターフェイスに接続します。
2. Configuration > Security > ACLの順に選択します。
3. すべてのトラフィックを拒否する新しいIPv6拡張ACLを追加します。

次に、Identity Services Engine(ISE)で次の操作を実行します。

1. Web管理インターフェイスに接続します。
2. Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に選択します。
3. CWAに使用される認可プロファイルを選択します。
4. Common Tasksの下にあるAirespace IPv6 ACL Nameに、前のステップで設定したACL名を入力します。

IPv4 ACLの追加

ワイヤレスコントローラに設定されているリダイレクションACLがIPv6 ACLである場合、すべてのトラフィックを拒否する新しいIPv4 ACLを作成し、CWA認証フェーズで適用する必要があります。これを行うには、次の手順を実行します。

まず、ワイヤレスコントローラで次の操作を実行します。

1. Web管理インターフェイスに接続します。
2. Configuration > Security > ACLの順に選択します。
3. すべてのトラフィックを拒否する新しいIPv4拡張ACLを追加します。

次に、ISEで次の操作を実行します。

1. Web管理インターフェイスに接続します。
2. Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に選択します。
3. CWAに使用される認可プロファイルを選択します。
4. Common Tasksの下のAirespace ACL Nameに、前のステップで設定したACL名を入力します。

この回避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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（15.9(3)M2、17.3.3 など）を入力します。
3. [チェック（Check）] をクリックします。

2 | | Critical,High,Medium

このアドバイザのみ

Enter release number | Check

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

出典

この脆弱性は Cisco TAC 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-c9800-cwa-acl-nPSbHSnA

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9月25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。