Cisco SD-WAN vEdgeソフトウェアのアクセスコントロールリストバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-defaultacl-pSJk9nVF
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwo83136

CVE-2025-20339

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 SD-WAN vEdgeソフトウェアのIPv4パケットのアクセスコントロールリスト(ACL)処理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設定されたACLをバイパスできる可能性があります。

この脆弱性は、設定されたACLの最後の暗黙的なdeny allが不適切に適用されることに起因します。攻撃者は、該当デバイスのインターフェイスに不正なトラフィックを送信しようとすることで、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、攻撃者は該当デバイスのACLをバイパスでき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-defaultacl-pSJk9nVF

該当製品

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、Cisco SD-WAN vEdgeソフトウェアの脆弱性のあるリリースを実行するCisco SD-WAN vEdgeルータがこの脆弱性の影響を受けました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新

の情報については、このアドバイザリの上部にあるバグ ID の詳細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。

- Catalyst SD-WAN Manager（旧称SD-WAN vManage Software）
- IOS XE ソフトウェア
- IOS XE SD-WAN ソフトウェア
- NX-OS ソフトウェア

詳細

この脆弱性がエクスプロイトされると、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。この脆弱性の悪用による影響はACLで保護されるはずの資産の重要性に依存しているため、全体として組織に固有です。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、お客様自身の脆弱性処理および修復プロセスに従って処理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はありません。管理者は、各自のニーズに最適なACLを決定し、インターフェイス上でその単一のACLタイプを設定する必要があります。

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。このアドバイザリの先頭にあるバグ

IDの詳細情報のセクションで、最新の情報を確認してください。

左側の列にはシスコソフトウェアリリース、右側の列に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リリースが示されています。

Cisco SD-WAN vEdge ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
20.8 以前	脆弱性なし
20.9	20.9.7
20.10 以降	脆弱性なし

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 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

この脆弱性は、Cisco Technical Assistance Center(TAC)の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-defaultacl-pSJk9nVF

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9月24日

利用規約

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。