Cisco Catalyst 9500Xおよび9600Xシリーズスイッチ上のCisco IOS XEソフトウェアにおける仮想インターフェイスアクセスコントロールリスト(VACL)バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-cat9k-acl-L4K7VXgD
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCwo11541

CVE-2025-20316

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 Catalyst 9500Xおよび9600Xシリーズスイッチ用Cisco IOS XEソフトウェアのアクセスコントロールリスト(ACL)プログラミングの脆弱性により、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、出力ACLが適用されたスイッチ仮想インターフェイス(SVI)上の未学習MACアドレスからのトラフィックのフラッディングに起因します。攻撃者は、VLANにMACアドレステーブルをフラッシュさせることで、この脆弱性を不正利用する可能性があります。この状況は、MACアドレステーブルがいっぱいになった場合にも発生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で出力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-cat9k-acl-L4K7VXgD

このアドバイザリは、Cisco IOS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2025年9月リリースの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年9月）』を参照してください。

該当製品

脆弱性のある製品

公開時点では、Cisco Catalyst 9500Xおよび9600Xシリーズスイッチで、脆弱性が存在するCisco IOS XEソフトウェアリリースが実行されており、出力ACLがSVIで設定されている場合、この脆弱性の影響を受けました。

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。

デバイス設定の確認

SVIで発信ACLが設定されているかどうかを確認するには、show running-config | include interface Vlan|out$コマンドを使用します。次の例は、SVIで出力ACLが設定されているデバイスでの出力を示しています。

<#root>

```
Switch# Router#
```

show running-config | include interface Vlan|out$

```
interface Vlan1
 ip access-group 101 out
Switch#
```

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 9500 シリーズ スイッチ
- Catalyst 9600 シリーズ スイッチ
- IOS ソフトウェア
- IOS XR ソフトウェア
- NX-OS 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。 出力ACLは入力ACLに変換できます。ただし、出力

ACLを使用して設定されているインターフェイスの数によっては、必要な設定変更が膨大なものになる可能性があります。

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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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（例：15.9(3)M2、17.3.3）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 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-cat9k-acl-L4K7VXgD

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

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。