Cisco Catalyst 1000および2960Lスイッチ上のCisco IOSソフトウェアにおけるアクセスコントロールリストのバイパスに関する脆弱性

アドバイザリーID : cisco-sa-ipsgacl-pg6qfZk
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 4.7
回避策 : Yes
Cisco バグ ID : CSCwm03838

CVE-2025-20137

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 1000スイッチおよびCisco Catalyst 2960Lスイッチで実行されているCisco IOS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、同じインターフェイス上でIPv4 ACLとIPソースガードのダイナミックACLの両方を使用していることに起因します。この設定はサポートされていません。攻撃者は、該当デバイスを介して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。

注：シスコのドキュメントは、この設定がサポート対象外であることを反映するように更新されています。ただし、管理者が同じインターフェイスで両方の機能を設定することをデバイスが妨げないため、このアドバイザリは公開されています。Cisco Catalyst 1000またはCatalyst 2960Lスイッチの同じインターフェイスで両方の機能を設定する機能を実装する計画はありません。

シスコでは、本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せん。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-ipsgacl-pg6qfZk

該当製品

脆弱性のある製品

公開時点では、次のシスコ製品で脆弱性のあるCisco IOSソフトウェアリリースが実行されており、インターフェイスにIPv4 ACLとIPソースガードの両方が設定されている場合に、この脆弱性の影響を受けました。

- Catalyst 1000 スイッチ
- Catalyst 2960-L シリーズ スイッチ

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

IPソースガードを使用している同じインターフェイスにデバイスのIPv4 ACLが設定されているかどうかを確認するには、show running-config CLIコマンドを使用します。各インターフェイスの下の内容を調べて、IPv4アクセスグループが、IPソースガードとともに設定されているかどうかを確認します。この設定は、次の例に示すように、ip verify sourceコマンドで有効になります。

<#root>

```
Switch#
show running-config
.
.
<output omitted>
.
.
interface GigabitEthernet1/0/11
switchport access vlan 200
ip access-group
 DropACL in
ip verify source

.
.
<output omitted>
.
.
Switch#
```

注：IP Source Guardの設定を有効にするには、IP Source GuardおよびIP access-groupが適用

されているVLANで、IP DHCPスヌーピングを有効にする必要があります。次の例は、VLAN 200でDHCPが有効になっていることを示しています。

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
200
DHCP snooping is operational on following VLANs:
200
.
.
.
output omitted
```

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。

- 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ないプラットフォームで実行されているIOSソフトウェア
- IOS XE 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

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全体的な影響は、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、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。

IPv4 ACLがアクティブになるか、IPソースガード用に動的に生成されたACLがアクティブになるかのどちらかです。ただし、両方は同時にアクティブになりません。プログラミングはコマンドの順序によって異なり、IPソースガードに変更があれば、ACLが更新されてIPソースガードACLが反映されます。

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

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完全なアップグレード ソリューション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。

修正済みリリース

この脆弱性はサポートされていない機能に影響を与えるため、シスコでは修正済みソフトウェアのリリースを計画していません。

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-ipsgacl-pg6qfZk

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5月7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。