Cisco IOS XRソフトウェアのアクセスコントロールリスト(ACL)バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-modular-ACL-u5MEPXMm
CVE-2025-20145
初公開日 : 2025-03-12 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwk63613 CSCwk94942

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 IOS XRソフトウェアの出力方向におけるアクセスコントロールリスト(ACL)処理の脆弱性により、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、あるラインカードの入力インターフェイスで受信されたパケットが、出力ACLが設定されている別のラインカードの出力インターフェイスを宛先とするパケットの場合に、正しく処理されないことに起因しています。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出力ACLをバイパスできる可能性があります。

この脆弱性の詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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。こ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-modular-ACL-u5MEPXMm

このアドバイザリは、Cisco IOS XRソフトウェアSecurity Advisoryバンドル公開の2025年3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 XRソフトウェアセキュリティアドバイザリバンドル公開の半年刊2025年3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、次のシスコ製品で脆弱性が存在するCisco IOS XRソフトウェアリリースが実行されており、出力IPv4またはIPv6パケットフィルタリングが有効にされている場合に、この脆弱性の影響を受けました。

- 8000シリーズモジュラプラットフォーム：次のモデルのみ。
  - 8608ルータ
  - 8804ルータ
  - 8808ルータ
  - 8812ルータ
  - 8818ルータ
- IOSXRWBDモジュラバリアント（分散分散シャーシ）
- Network Convergence System(NCS)5500モジュラプラットフォーム：次のモデルのみ。
  - NCS S5504
  - NCS S5508
  - NCS S5516

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。

出力方向でIPパケットフィルタリングが有効になっているかどうかを確認する

出力IPv4またはIPv6 ACLが設定されているかどうかを確認するには、show running-config | include ipv4 access-group .* egressまたはshow running-config | include ipv6 access-group .* egress CLIコマンドを使用します。コマンドの出力が返された場合は、次の例に示すように、機能が設定されています。

```
<#root>

RP/0/RP0/CPU0:NCS-5508-A#

show running-config | include ipv4 access-group .* egress


Wed Mar  12 16:00:00.000 UTC
Building configuration...


ipv4 access-group

 EgressACL
```

```
egress

RP/0/RP0/CPU0:NCS-5508-A#
```

```
<#root>

RP/0/RP0/CPU0:NCS-5508-A#

show running-config | include ipv6 access-group .* egress

Wed Mar  12 16:00:00.000 UTC
Building configuration...

ipv6 access-group

 EgressACL

egress

RP/0/RP0/CPU0:NCS-5508-A#
```

注：Bridged Virtual Interface(BVI)を除くすべてのインターフェイス出力タイプが影響を受けます。

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。

- IOS ソフトウェア
- IOS XE 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。

該当する製品では、入力インターフェイスで受信され、（ACLが適用されている）別のラインカードの出力インターフェイスを宛先とするトラフィックに対して、入力インターフェイスで受信

され、出力インターフェイスから送信される特定のパケットが、設定された出力ACLの対象にはなりません。

入力インターフェイスで受信され、同じラインカード上の出力インターフェイスを宛先とするトラフィックは、この脆弱性の影響を受けません。入力インターフェイスと出力インターフェイスが同じラインカード上にある場合、出力ACLは適切に処理されます。

回避策

この脆弱性に対処する回避策はありません。

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

発行時点では、次の表に記載されているリリース情報は正確でした。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。

次の表では、左の列にシスコ ソフトウェア リリースまたはトレインを記載しています。右側の列は、リリース（トレイン）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最初のリリースを示しています。

8000シリーズモジュラプラットフォーム

Cisco IOS XR 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）
24.4 以前	修正済みリリースに移行。
25.1.1 以降	影響なし。

NCS 5500モジュラプラットフォーム

Cisco IOS XR 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）
7.10 以前	修正済みリリースに移行。
7.11	7.11.21
24.1	修正済みリリースに移行。

Cisco IOS XR 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）
24.2	24.2.2
24.3 以降	影響なし。

この脆弱性に対処するためにSMUも使用できます。使用できないプラットフォームまたはリリースでSMUを必要とするお客様は、サポート組織に連絡することをお勧めします。この脆弱性に対して公開されている可能性があるSMUを見つける方法の詳細については、『Cisco IOS XRソフトウェアメンテナンスアップデート(SMU)について』の「ダウンロード」セクションを参照してください。

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 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 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-modular-ACL-u5MEPXMm

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3月12日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
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。