Cisco IOS XRソフトウェア管理インターフェイスのACLバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-acl-packetio-Swjhhbtz
CVE-2025-20159
初公開日 : 2025-09-10 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCwb70861 CSCwo52518 CSCwo51041 CSCwq48170

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ソフトウェアの管理インターフェイスアクセスコントロールリスト(ACL)処理機能の脆弱性により、認証されていないリモートの攻撃者が、SSH、NetConf、およびgRPC機能に対して設定されたACLをバイパスできる可能性があります。

この脆弱性は、Cisco IOS XRソフトウェアのパケットI/Oインフラストラクチャプラットフォームでは、SSH、NetConf、gRPCなどのLinuxで処理される機能に対して管理インターフェイスACLがサポートされていないことに起因しています。攻撃者は、該当デバイスに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管理インターフェイスに適用されている入力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。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-acl-packetio-Swjhhbtz

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 XR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、次のシスコプラットフォームおよびCisco IOS XRソフトウェアリリースで、管理インターフェイスにIPv4またはIPv6 ACLが接続されている場合、この脆弱性の影響を受けます。

該当するシスコプラットフォーム	該当するCisco IOS XRソフトウェアリリース
8000 シリーズ ルータ	最初の修正リリースより前のソフトウェアイメージ
ASR 9000 シリーズ アグリゲーション サービス ルータ	リリース24.1.1以降で、最初の修正済みリリースよりも前
IOS XR ホワイトボックス（IOSXRWBD）	リリース7.9.1以降で、最初の修正済みリリースよりも前
IOS XRd vRouter	最初の修正リリースより前のソフトウェアイメージ
IOS XRv 9000 ルータ	リリース24.1.1以降で、最初の修正済みリリースよりも前
Network Convergence Series(NCS)540シリーズルータ （NCS540-iosxrベースイメージ）	リリース7.9.1以降で、最初の修正済みリリースよりも前
NCS 540 シリーズ ルータ （NCS540L-iosxrベースイメージ）	最初の修正済みリリースより前のすべてのリリース
NCS 560 シリーズ ルータ	リリース24.2.1以降で、最初の修正済みリリースよりも前
NCS 1010プラットフォーム	最初の修正リリースより前のソフトウェアイメージ
NCS 1014プラットフォーム	最初の修正リリースより前のソフトウェアイメージ
NCS 5500 シリーズ ルータ	リリース7.9.1以降で、最初の修正済みリリースよりも前
NCS 5700 シリーズ ルータ	NCS5700の最初の修正リリースより前のベースイメージ

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の詳細については、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。

設定に脆弱性があるかどうかを確認する

上の表のデバイスに脆弱性のある設定があるかどうかを確認するには、次の手順に従います。

ステップ1:IP ACLがあるかどうかを確認する

デバイスの管理インターフェイス上にIP ACLが設定されていて、そのACLがgRPC、SSH、またはNETCONF over SSHをブロックするように設定されているかどうかを確認するには、show running-config interface mgtEth <value> CLIコマンドを使用します。次の例は、管理インターフェイスでIPv4 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>

RP/0/RP0/CPU0:Router#

show running-config interface mgmtEth 0/RP0/CPU0/0


Wed Sep 9 16:00:00.000 UTC

interface MgmtEth

0/RP0/CPU0/0
ipv4 address 10.10.10.10 255.255.255.0
i

pv4 access-group

 MGMT_ACL ingress
!

RP/0/RP0/CPU0:Router#
```

MGMT_ACLの内容を調べます。gRPC、SSH、またはNETCONF over SSHが設定されたポートを拒否するように設定されている場合、これは一致します。ステップ 2 に進みます。

それ以外の場合、デバイスは影響を受けません。ここで止まって。

ステップ2:gRPCのステータスを判別する

デバイスでgRPCが設定されているかどうかを確認するには、show running-config grpc CLIコマンドを使用します。次の例は、gRPCが有効で設定されているデバイスでの出力を示しています。

```
<#root>

RP/0/RP0/CPU0:Router#
```

```
show running-config grpc

Wed Sep 9 16:00:00.000 UTC
grpc

port 57400
!
RP/0/RP0/CPU0:Router#
```

gRPCが有効になっている場合は、CLIコマンドshow running-config linux networkingを使用してLinuxネットワークのトラフィック保護が設定されているかどうかを確認します。次の例は、単一のローカルインターフェイス上の単一のリモートサブネットからのgRPCのみを許可するデバイスの出力を示しています。

```
<#root>
RP/0/RP0/CPU0:Router#
show running-config linux networking

Wed Sep 9 16:00:00.000 UTC
linux networking
 vrf default
  address-family ipv4
   protection
    protocol tcp local-port all default-action deny
    !
    protocol tcp local-port 57400 default-action deny
     permit remote-address 192.0.2.0/24 interface HundredGigE0/0/0/25
    !
   !
  !
!
RP/0/RP0/CPU0:Router#
```

gRPCが有効で、トラフィック保護がgRPCサービスを保護するように設定されている場合、デバイスは正しく設定されています。

gRPCが有効になっているが、トラフィック保護がgRPCサービスを保護するように構成されていない場合は、トラフィック保護を構成するか、固定リリースに移行してgRPCの管理インターフェイスフィルタリングサポートを利用します。

次のシスコ製品およびリリースを評価する場合のみ、ステップ3に進んでください。

- 最初の修正済みリリースより前のIOS XRイメージを実行している8000シリーズルータ
- 最初の修正済みリリースより前のNCS540L-iosxrベースイメージを実行しているNCS

540シリーズルータ
- 最初の修正済みリリースより前のNCS5700ベースイメージを実行しているNCS 5700シリーズルータ

それ以外の場合は、ここで停止します。

ステップ3:SSHのステータスを確認する

デバイスでSSHが設定されているかどうかを確認するには、show running-config ssh CLIコマンドを使用します。次の例は、SSHサービスが有効で設定されているデバイスでの出力を示しています。この例では、デバイスにIPv4 ACLとIPv6 ACLの両方がSSHサーバに対して設定されています。

```
<#root>

RP/0/RP0/CPU0:Router#

show running-config ssh


Wed Sep 9 16:00:00.000 UTC

ssh server v2
ssh server

 vrf mgmt

ipv4 access-list

SSH_ACL_Ingress

ipv6 access-list

 SSH_ACL_Ingress

RP/0/RP0/CPU0:Router#
```

SSHが有効で、IP ACLがSSHサービスに適用されている場合、デバイスは正しく設定されています。

SSHが有効でも、SSHサービスを保護するようにIP ACLが設定されていない場合は、ssh server ipv4|ipv6 access-list <name>設定を追加するか、修正済みリリースに移行してSSHの管理インターフェイスフィルタリングサポートを利用します。

ステップ 4 に進みます。

ステップ4:SSH経由のNETCONFのステータスを確認する

NETCONF over SSHが設定されているかどうかを確認するには、show running-config ssh server netconf CLIコマンドを使用します。次の例は、NETCONF over SSHが有効で設定され

ているデバイスでの出力を示しています。この例では、デバイスにIPv4 ACLとIPv6 ACLの両方がNetConf SSHサーバに対して設定されています。

<#root>

```
RP/0/RP0/CPU0:Router#show running-config ssh server netconf
Wed Sep 9 16:00:00.000 UTC
ssh server netconf
 vrf mgmt
ipv4 access-list
 NetConf_ACL_Ingress
ipv6 access-list
 NetConf_ACL_Ingress
RP/0/RP0/CPU0:Router#
```

NETCONF over SSHが有効で、NETCONF SSHサービスにIP ACLが適用されている場合、デバイスは正しく設定されています。

NETCONF over SSHが有効でも、NETCONF SSHサービスを保護するようにIP ACLが設定されていない場合、ssh server netconf ipv4|ipv6 access-list <name>設定を追加するか、修正済みリリースに移行して、NETCONF SSHの管理インターフェイスフィルタリングサポートを利用します。

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

Cisco IOS XRソフトウェアパケットI/Oインフラストラクチャは、次のシスコプラットフォーム（ネイティブパケットI/Oプラットフォーム）で実行されているすべてのリリースで使用されます。

- 8000 シリーズ ルータ

- IOS XRd vRouter
- NCS 540シリーズルータ（NCS540Lベースイメージ）
- ncs 1010プラットフォーム[1]
- ncs 1014プラットフォーム[1]
- NCS 5700シリーズルータ（NCS5700ベースイメージ）

1. Cisco NCS 1010およびNCS 1014プラットフォームでは、ソフトウェアGigabitEthernet0/0/0/[0-3]インターフェイス経由で着信するトラフィックを管理トラフィックインターフェイスと見なします。そのため、ACLが適用される場合、mgmtEthインターフェイスと同じ条件の対象となります。

次のプラットフォームは、指定されたリリースでパケットI/Oインフラストラクチャに移行しました（移行されたパケットI/Oプラットフォーム）。

- ASR 9000シリーズアグリゲーションサービスルータ：24.1.1以降
- IOS XRホワイトボックス(IOSXRWBD):7.9.1以降
- IOS XRv 9000ルータ：24.1.1以降
- NCS 540シリーズルータ：7.9.1以降
- NCS 560シリーズルータ：24.2.1以降
- NCS 5500シリーズルータ：7.9.1以降

Cisco IOS XRソフトウェアのパケットI/Oインフラストラクチャでは、管理インターフェイスに適用されるACLは、どのLinuxアプリケーションにも適用されません。これには、gRPC、SSH(CiscoSSH)、NETCONF、および顧客がインストールしたLinuxアプリケーションが含まれます。

ネイティブパケットI/Oプラットフォーム

このセクションには、管理インターフェイスACLをサポートしていないリリースに関する詳細が含まれています。

gRPC

gRPCサービスのフィルタリングは、Linuxネットワーキングのトラフィック保護を使用して行う必要があります。詳細については、『Cisco IOS XRソフトウェア強化ガイド』の「トラフィック保護のベストプラクティス」セクションを参照してください。

Linuxネットワークのトラフィック保護は、確立された接続に一致しない着信トラフィックから保護し、発信トラフィックからは保護しません。

入力管理インターフェイスACLによるgRPCのフィルタリングは、Cisco IOS XRソフトウェアリリース25.1.2以降およびリリース25.2.1以降からのみサポートされています。この問題は、Cisco Bug ID CSCwo52518に記載されています。

SSHおよびNETCONF over SSH

これらのプラットフォームでは、Linuxネットワーキングで処理されるCiscoSSHが使用されます。Linuxネットワーキングのトラフィック保護は、CiscoSSHを対象としていません。

入力SSHおよびNetconfトラフィックをフィルタリングして除外するには、SSHサーバ設定モードで入力ACLを設定することをお勧めします。

- SSHの場合：ssh server vrf vrf-name ipv4 access-list ipv4-access-list-name ipv6 access-list ipv6-access-list-name
- Netconfの場合：ssh server netconf vrf vrf-name ipv4 access-list ipv4-access-list-name ipv6 access-list ipv6-access-list-name

入力管理インターフェイスACLを使用したSSHおよびNetconf over SSHのフィルタリングは、Cisco IOS XRソフトウェアリリース25.1.1以降からのみサポートされています。この問題は、Cisco Bug ID CSCwb70861に記載されています。

Cisco IOS XRソフトウェアリリース25.1.1以降では、SSHおよびNetConfトラフィック用の管理インターフェイスでフィルタリングを設定する場合、管理者はssh server packet-flow-netio ingressを設定する必要があります。

移行されたパケットI/Oプラットフォーム

gRPC

パケットI/Oをサポートするリリースにプラットフォームが移行されたら、Cisco IOS XRソフトウェア強化ガイドの「Linuxネットワーキング用のトラフィック保護」セクションの手順を使用してgRPCサービスのフィルタリングを行う必要があります。

パケットI/Oインフラストラクチャに移行されたこのセクションの上部に記載されているプラットフォーム上の管理インターフェイスに適用される入力ACLによるgRPCのフィルタリングは、Cisco IOS XRソフトウェアリリース24.2.21以降、リリース25.1.2以降、およびリリース25.2.1以降でサポートされています。この問題は、Cisco Bug ID CSCwo51041に記載されています。

SSHおよびNETCONF over SSH

公開時点では、このセクションの最上部に掲載されているプラットフォームで使用されているSSHサービスは、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ません。

フィルタリングは、SSHサーバコンフィギュレーションモードまたは入力管理インターフェイスACLを介してサポートされます。

回避策

IPv4またはIPv6 ACLを管理インターフェイスに接続してgRPC、SSH、またはNETCONF over

SSHをブロックする回避策はありません。お客様は、この機能のサポートが導入された修正済みリリースに移行する必要があります。デバイスを不正アクセスから適切に保護するために影響を受けるプロトコルに適用するフィルタリングのプラットフォームとタイプの詳細については、このアドバイザリの「詳細」セクションを参照してください。

ただし、修正済みリリースにアップグレードできないお客様は、この脆弱性に対する回避策を使用できます。回避策の実装の調整に関しては、 Cisco Technical Assistance Center（TAC）にお問い合わせください。

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

公開時点では、次の表の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。中央と右側の列は、リリース（トレイン）がこのアドバイザリに記載された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。

シスコ プラットフォーム	管理インターフェイス ACL(gRPC)をサポートする最初の修正済みリリース	管理インターフェイス ACLをサポートする最初の修正済みリリース – SSHおよびNETCONF
8000シリーズルータ[1]	25.1.2 25.2.1	25.1.1
ASR 9000 シリーズ アグリゲーション サービス ルータ	24.2.21 25.1.2	Not affected

シスコ プラットフォーム	管理インターフェイス ACL(gRPC)をサポートする最初の修正済みリリース	管理インターフェイス ACLをサポートする最初の修正済みリリース – SSHおよびNETCONF
	25.2.1	
IOS XR ホワイトボックス（IOSXRWBD）	24.2.21 25.1.2 25.2.1	Not affected
IOS XRd vRouter	25.1.2 25.2.1	25.1.1
IOS XRv 9000 ルータ	24.2.21 25.1.2 25.2.1	Not affected
NCS 540 シリーズ ルータ（NCS540-iosxrベースイメージ）	24.2.21 25.1.2 25.2.1	Not affected
NCS 540 シリーズ ルータ（NCS540L-iosxrベースイメージ）	25.1.2 25.2.1	25.1.1
NCS 560 シリーズ ルータ	24.2.21 25.1.2 25.2.1	Not affected
NCS 1010プラットフォーム	25.1.2 25.2.1	25.1.1
NCS 1014プラットフォーム	25.1.2 25.2.1	25.1.1
NCS 5500 シリーズ ルータ	24.2.21 25.1.2 25.2.1	Not affected
NCS 5700 シリーズ ルータ	25.1.2 25.2.1	25.1.1

1. デュアルルートプロセッサを使用するCisco 8000の展開では、スタンバイルートプロセッサの管理インターフェイスでのフィルタリングが正しく適用されません。デュアルルートプロセッサを使用しているお客様は、アクティブおよびスタンバイの両方のルートプロセッサでフィルタリングが正しく適用されていることを確認できる場合は、リリース25.2.2、25.4.1、または26.1.1に移行する必要があります。この問題は、Cisco Bug ID CSCwq48170に記載されています。

デバイスを保護するための適切な代替設定が用意されているため、この脆弱性に対して使用できるSMUはありません。管理インターフェイスに設定されたACLでこれらのプロトコルのサポートを必要とするお客様は、修正済みのソフトウェアリリースにアップグレードする必要があります

。

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 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-acl-packetio-Swjhhbtz

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10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。