Cisco IOS XRソフトウェアのハイブリッド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-ncs-hybridacl-crMZFfKQ　CVE-2025-20144
初公開日 : 2025-03-12 16:00
バージョン 1.0 : Final
CVSSスコア : 4.0
回避策 : Yes
Cisco バグ ID : CSCwi49569

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ソフトウェアにおけるIPv4パケットのハイブリッド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、ハイブリッドACLの特定の設定が存在する場合のパケットの不適切な処理に起因します。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で設定されているACLをバイパスできる可能性があります。

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-ncs-hybridacl-crMZFfKQ

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、次の製品で脆弱性のあるCisco IOS XRソフトウェアリリースが実行されており、特定の特性に一致するcompressレベル3が設定されたハイブリッドIPv4 ACLが存在する場合に、この脆弱性の影響を受けました。

- IOS XR ホワイトボックス（IOSXRWBD）
- Network Convergence Series(NCS)540シリーズルータ
- NCS 560 シリーズ ルータ
- NCS 5500 シリーズ
- NCS 5700 シリーズ

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。

ハイブリッドIPv4 ACLの脆弱性の確認

1. デバイスにハイブリッドACLが設定されているかどうかを確認します。

ハイブリッドIPv4 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 .* compress level 3 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、ハイブリッドIPv4 ACLが設定されています。

<#root>

```
RP/0/RP0/CPU0:Router#
show running-config | include ipv4 access-group .* compress level 3

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

ipv4 access-group
 IngressACL ingress
 compress level 3

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

設定されていない場合、デバイスはこの脆弱性の影響を受けません。

設定されている場合は、ステップ2に進みます。

2. ACLを調べます。

前の手順で特定された各ハイブリッドACLの内容を調べるには、show access-list <ACLの名前> CLIコマンドを使用します。異なるソースネットワークオブジェクトグループの数が32以上の場合、または異なる宛先ネットワークオブジェクトグループの数が32以上の場合は、手順3に進みます。32未満の数の場合、ACLはこの脆弱性の影響を受けません。

次の例は、33個の一意の送信元ネットワークオブジェクトグループと33個の一意の宛先ネットワークオブジェクトグループを持つ33個のアクセスコントロールエントリ(ACE)を示しています。

```
RP/0/RP0/CPU0:Router#show access-lists CSCwi49569_long
Wed Mar  12 16:00:00.000 UTC
ipv4 access-list CSCwi49569_long
 400000 permit ipv4 net-group 1_SRC_100 net-group 1_DST_100
 400001 permit ipv4 net-group 1_SRC_101 net-group 1_DST_101
 400002 permit ipv4 net-group 1_SRC_102 net-group 1_DST_102
 400003 permit ipv4 net-group 1_SRC_103 net-group 1_DST_103
 400004 permit ipv4 net-group 1_SRC_104 net-group 1_DST_104
 400005 permit ipv4 net-group 1_SRC_105 net-group 1_DST_105
 400006 permit ipv4 net-group 1_SRC_106 net-group 1_DST_106
 400007 permit ipv4 net-group 1_SRC_107 net-group 1_DST_107
 400008 permit ipv4 net-group 1_SRC_108 net-group 1_DST_108
 400009 permit ipv4 net-group 1_SRC_109 net-group 1_DST_109
 400010 permit ipv4 net-group 1_SRC_110 net-group 1_DST_110
 400011 permit ipv4 net-group 1_SRC_111 net-group 1_DST_111
 400012 permit ipv4 net-group 1_SRC_112 net-group 1_DST_112
 400013 permit ipv4 net-group 1_SRC_113 net-group 1_DST_113
 400014 permit ipv4 net-group 1_SRC_114 net-group 1_DST_114
 400015 permit ipv4 net-group 1_SRC_115 net-group 1_DST_115
 400016 permit ipv4 net-group 1_SRC_116 net-group 1_DST_116
 400017 permit ipv4 net-group 1_SRC_117 net-group 1_DST_117
 400018 permit ipv4 net-group 1_SRC_118 net-group 1_DST_118
 400019 permit ipv4 net-group 1_SRC_119 net-group 1_DST_119
 400020 permit ipv4 net-group 1_SRC_120 net-group 1_DST_120
 400021 permit ipv4 net-group 1_SRC_121 net-group 1_DST_121
 400022 permit ipv4 net-group 1_SRC_122 net-group 1_DST_122
 400023 permit ipv4 net-group 1_SRC_123 net-group 1_DST_123
 400024 permit ipv4 net-group 1_SRC_124 net-group 1_DST_124
 400025 permit ipv4 net-group 1_SRC_125 net-group 1_DST_125
 400026 permit ipv4 net-group 1_SRC_126 net-group 1_DST_126
 400027 permit ipv4 net-group 1_SRC_127 net-group 1_DST_127
 400028 permit ipv4 net-group 1_SRC_128 net-group 1_DST_128
 400029 permit ipv4 net-group 1_SRC_129 net-group 1_DST_129
 400030 permit ipv4 net-group 1_SRC_130 net-group 1_DST_130
 400031 permit ipv4 net-group 1_SRC_131 net-group 1_DST_131
 400032 permit ipv4 net-group 1_SRC_132 net-group 1_DST_132
RP/0/RP0/CPU0:Router#
```

3. オブジェクトグループを確認します。

コマンドが32以上の異なる送信元ネットワークオブジェクトグループまたは32以上の異なる宛

先ネットワークオブジェクトグループを含む出力を返す場合、前のステップからshow object-group network ipv4 <name of each network object-group> CLIコマンドを使用して、各ACEに表示される各グループの内容を調べる必要があります。

同じIPv4プレフィックス、ホスト、または範囲エントリが、32以上の送信元ネットワークオブジェクトグループまたは32以上の宛先ネットワークオブジェクトグループで見つかった場合、ACLはこの脆弱性の影響を受けます。

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。

回避策

この脆弱性に対処する回避策はありません。

ACLを構成するオブジェクトグループを調べます。同じIPv4送信元または宛先あるいはその両方が、ACLを構成するオブジェクトグループに31回以上ある場合、同じIPv4アドレスのエントリが送信元と宛先の両方に31個以下になるまで、アクセスコントロールエントリ(ACE)を削除します。

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

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。

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	7.11.2
24.1 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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ncs-hybridacl-crMZFfKQ

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

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。