Cisco IOS XRソフトウェアのMPLSおよび擬似回線インターフェイスにおける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-iosxr-acl-bypass-RZU5NL3e
初公開日 : 2024-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwh77265 CSCwf99658

CVE-2024-20322
CVE-2024-20315

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MPLSおよび擬似回線(PW)インターフェイスにおける入力方向のIPアクセスコントロールリスト(ACL)処理における複数の脆弱性により、認証されていないリモートの攻撃者が設定済みのACLをバイパスできる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。CVE-2024-20315に対処する回避策があります。CVE-2024-20322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-iosxr-acl-bypass-RZU5NL3e

このアドバイザリは、2024年3月に公開された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の一部です。アドバイザリとリンクの一覧については、Cisco Event Response: March 2024 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication 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、これらの脆弱性は、Cisco IOS XRソフトウェアの脆弱性が存在するリリースを実行し、MPLSまたはPW-Etherインターフェイスの入力方向でIPパケットフィルタリングを有効にしている次のシスコ製品に影響を与えました。

- 8000 シリーズ ルータ
- 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

注：MPLSインターフェイスでのIP入力ACLフィルタリングは、他のCisco IOS XRプラットフォームでは現在サポートされていません。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。

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の確認

MPLSインターフェイス – CVE-2024-20315

いずれかのMPLSインターフェイスで入力方向の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には、次の手順を実行します。

1.すべてのMPLSインターフェイスの特定

すべてのMPLSインターフェイスを識別するには、show mpls interfaces CLIコマンドを使用して、Enabled列でYesが表示されているインターフェイスを探します。

次の例は、インターフェイスTenGigE0/0/0/0およびTenGigE0/0/0/1でMPLSが有効になっているデバイスでのshow mpls interfacesコマンドの出力を示しています。

```
<#root>

RP/0/RP0/CPU0:NCS5501#

show mpls interfaces


Tue Jan 16 02:47:56.142 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------
TenGigE0/0/0/0             No       No       No

Yes


TenGigE0/0/0/1             No       No       No
```

```
Yes

RP/0/RP0/CPU0:NCS5501#
```

2.インターフェイスIPパケットフィルタリング設定の決定

インターフェイスに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 interface if_name CLIコマンドを使用します。

次の例は、入力方向のインターフェイスTenGigE0/0/0/0にIPv4とIPv6 ACLの両方が設定されているデバイスでのshow running-config interface TenGigE0/0/0/0コマンドの出力を示しています。

```
<#root>
RP/0/RP0/CPU0:NCS5501#
show running-config interface
TenGigE0/0/0/0
Tue Jan 16 02:49:45.385 UTC
interface TenGigE0/0/0/0
 description ** Example where IPv4 and IPv6 ACL ingress applied **
 ipv4 address 192.168.12.1 255.255.255.0

ipv4 access-group
 INGRESS_MPLS_IPV4_ACL
ingress


ipv6 access-group
 INGRESS_MPLS_IPV6_ACL
ingress

!
RP/0/RP0/CPU0:NCS5501#
```

少なくとも1つのMPLSインターフェイスにIPv4またはIPv6（またはその両方）の入力ACLが適用されている場合、デバイスはこの脆弱性の影響を受けます。

PW-Etherインターフェイス – CVE-2024-20322

任意のPW-Etherインターフェイスで入力方向の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には、次の手順を実行します。

1.すべてのPW-Etherインターフェイスの特定

すべてのPW-Etherインターフェイスを識別するには、show running-config | include ^interface PW-Ether CLIコマンドを使用します。

以下に、show running-config | include ^interface PW-Etherコマンドを、2つのPW-Etherインターフェイス PW-Ether1とPW-Ether2が設定されたデバイスで実行した場合の出力例を示します。

<#root>

```
RP/0/RP0/CPU0:NCS5501#
show running-config | include ^interface PW-Ether

Tue Jan 16 10:59:15.163 UTC
Building configuration...
interface
 PW-Ether1
interface
 PW-Ether2
RP/0/RP0/CPU0:NCS5501#
```

2.インターフェイスIPパケットフィルタリング設定の決定

show running-config interface if_name CLIコマンドを使用して、インターフェイスにIPv4またはIPv6 ACLが設定されているかどうかを確認します。

次の例は、入力方向のインターフェイスPW-Ether2にIPv4 ACLが設定されているデバイスでのshow running-config interface PW-Ether2コマンドの出力を示しています。

<#root>

```
RP/0/RP0/CPU0:NCS5501#
show running-config interface
 PW-Ether2
Tue Jan 16 11:16:42.356 UTC
interface PW-Ether2
 mtu 9000
 vrf vxlan2
 ipv4 address 196.168.48.1 255.255.255.0
 attach generic-interface-list txlist1
```

```
ipv4 access-group
 INGRESS_VXLAN_IPV4_ACL
ingress

!
RP/0/RP0/CPU0:NCS5501#
```

1つ以上のPW-EtherインターフェイスにIPv4またはIPv6（またはその両方）の入力ACLが適用されている場合、デバイス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記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に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

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

これらの脆弱性が不正利用されると、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。この脆弱性の全体的な影響は、ACLで保護する必要のある資産の重要性に依存するため、組織によって異なります。お客様は、これらの脆弱性の不正利用がネットワークにどのように影響するかを評価し、脆弱性の処理と修復のプロセスに従って作業を進める必要があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20315:Cisco IOS XRソフトウェアのMPLSインターフェイスにおけるアクセスコントロールリストバイパスの脆弱性

Cisco IOS XRソフトウェアの入力方向のMPLSインターフェイスにおける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、内部インターフェイスコンテキストへのルックアップキーの不適切な割り当てに

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、設定されたACLによって保護されているはずの該当デバイスの背後にあるリソースにアクセ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。

バグID:CSCwf99658
CVE ID：CVE-2024-20315
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVE-2024-20322:Cisco IOS XRソフトウェアの擬似回線インターフェイス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

Cisco IOS XRソフトウェアの入力方向の擬似回線インターフェイスにおける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、内部インターフェイスコンテキストへのルックアップキーの不適切な割り当てに起因します。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、設定されたACLによって保護されているはずの該当デバイスの背後にあるリソースにアクセ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。この脆弱性に対処する回避策はありません。

バグID:CSCwh77265
CVE ID：CVE-2024-20322
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

回避策

CVE-2024-20315:この脆弱性に対処する回避策があります。

お客様は、MPLS対応インターフェイスから入力ACLを削除し、代わりに環境で出力ACLを使用できます。出力ハイブリッドACLは、Cisco IOS XRリリース7.6.2以降でサポートされています。

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。

CVE-2024-20322: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アップグレード ソリューション一式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。

左側の列にはシスコソフトウェアリリース、右側の列にはリリース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リリースが示されています。

CVE-2024-20315

Cisco IOS XR ソフトウェア リリース	該当するリリース	First Fixed Release（修正された最初のリリース）
7.8 以前	脆弱性なし	脆弱性なし
7.9	7.9.1 および 7.9.2	修正済みリリースに移行。
7.10	7.10.1	7.10.2
7.11	脆弱性なし	脆弱性なし

CVE-2024-20322

Cisco IOS XR ソフトウェア リリース	該当するリリース	First Fixed Release（修正された最初のリリース）
7.9 以前	脆弱性なし	脆弱性なし
7.10	7.10.2	修正済みリリースに移行。

Cisco IOS XR ソフトウェア リリース	該当するリリース	First Fixed Release（修正された最初のリリース）
7.11	7.11.1	7.11.2

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

CVE-2024-20315：この脆弱性は、内部セキュリティテストで発見されました。

CVE-2024-20322：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-iosxr-acl-bypass-RZU5NL3e

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	2024年3月13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。