Cisco IOS XRソフトウェアの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-dnx-acl-PyzDkeYF
初公開日 : 2023-09-13 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwe63504

CVE-2023-20191

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ソフトウェアの入力方向のMPLSインターフェイス上のアクセスコントロールリスト(ACL)処理における脆弱性により、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、この機能のサポートが不完全であることに起因します。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のACLをバイパ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。

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-dnx-acl-PyzDkeYF

このアドバイザリは、2023年9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。これらのアドバイザリとそのリンクの一覧については、『Cisco Event Response: September 2023 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

公開時点では、この脆弱性は、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、入力方向のexplicit-nullまたはde-aggregationラベルでMPLS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。

- 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

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。

入力方向でのMPLSパケットのフィルタリングが有効になっているかどうかの確認

入力方向でMPLSパケットの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2ステップのプロセスに従います。

1. すべてのMPLSインターフェイスを特定します。
2. 設定をチェックして、入力方向に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、入力方向でIPv4とIPv6 ACLの両方が設定されているMPLSインターフェイスTenGigE0/0/0/0を示しています。show mpls interfacesで、Enabled列にYesが表示されている場合は、そのインターレースでMPLSが有効になっています。

```
<#root>

RP/0/RP0/CPU0:NCS5501-1##

show mpls interfaces


Thu Mar 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:NCS5501-1#
```

次の例に示すように、上の例のいずれかのインターフェイスにIPv4またはIPv6のいずれかの入力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。

```
<#root>
```

```
RP/0/RP0/CPU0:NCS5501-1#
show run interface TenGigE0/0/0/0

!
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
 CVE-2023-20191
ingress

ipv6 access-group
 CVE-2023-20191
ingress

!
RP/0/RP0/CPU0:NCS5501-1#
```

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。

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組織によって異なります。これは、ACLで保護する必要のある資産の重要性によって影響が異なるためです。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、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。

この脆弱性は、入力方向にexplicit-nullまたはde-aggregationラベルが付いたMPLSパケットのフィ

ルタリングが、どのCisco IOS XRプラットフォームでもサポートされていないことに起因しています。ただし、このアドバイザリの「脆弱性が存在する製品」セクションに記載されている製品に対するサポートが追加されています。該当するデバイスがラベル付きパケットを受信してラベルをポップすると、設定された入力ACLの処理を試みます。ACLの拒否エントリがヒットすると、パケットはパントされて、返されるICMP到達不能パケットが生成されます。このパスは、パケットをドロップするのではなく、拒否されたパケットを宛先に転送します。

回避策

この脆弱性に対処する回避策はありません。

お客様は、MPLS対応インターフェイスから入力ACLを削除し、環境内で出力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。

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。

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）
6.3 以前	影響なし。
6.4 ~ 6.6	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）
7.0 ~ 7.6	修正済みリリースに移行するか、利用可能なSMUを適用します。
7.7	7.7.21
7.8	修正済みリリースに移行。
7.9	7.9.2
7.10	7.10.1

シスコはこの脆弱性に対処するため、次のSMUをリリースしました。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.0.1	NCS5500	ncs5500-7.0.1.CSCwe63504（登録ユーザ専用）
7.2.1	IOSXRWBD	iosxrwbd-7.2.1.CSCwe63504
7.4.15	IOSXRWBD	iosxrwbd-7.4.15.CSCwe63504
7.7.2	IOSXRWBD	iosxrwbd-7.7.2.CSCwe63504
7.7.2	NCS540L	ncs540l-aarch64-7.7.2.CSCwe63504（登録ユーザ専用）
7.7.2	NCS5500	ncs5500-7.7.2.CSCwe63504（登録ユーザ専用）

注：次の表に記載されていないリリース向けの SMU を必要とするお客様は、サポート部門にご連絡ください。

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-dnx-acl-PyzDkeYF

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	2023-9-13

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。