ASR 9000シリーズルータIPv4ユニキャストパケット用Cisco IOS XRソフトウェアのサービス妨害(DoS)脆弱性

アドバイザリーID : cisco-sa-ipv4uni-LfM3cfBu
初公開日 : 2025-03-12 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwf56155

CVE-2025-20142

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 ASR 9000シリーズアグリゲーションサービスルータ、ASR 9902コンパクト高性能ルータ、およびASR 9903コンパクト高性能ルータ用Cisco IOS XRソフトウェアのIPv4アクセスコントロールリスト(ACL)機能およびQuality of Service(QoS)ポリシー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ラインカードをリセットさせ、その結果サービス妨害(DoS)状態が発生するするする可能性があります。

この脆弱性は、インターフェイスにIPv4 ACLまたはQoSポリシーが適用されているラインカードで受信された不正なIPv4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巧妙に細工されたIPv4パケットを送信することにより、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、攻撃者がネットワークプロセッサエラーを引き起こし、ネットワークプロセスがリセットまたはシャットダウンされる可能性があります。そのラインカードを経由するトラフィックは、ラインカードのリロード中に失われます。

注：この脆弱性は、主にレイヤ2 VPN(L2VPN)環境で確認されており、IPv4 ACLまたはQoSポリシーがブリッジ仮想インターフェイスに適用されています。脆弱性は確認されていませんが、インターフェイスにIPv4 ACLまたはQoSポリシーが適用されているレイヤ3設定も影響を受けます。

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。この脆弱性に対処する対応策があります。

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-ipv4uni-LfM3cfBu

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

この脆弱性は、Cisco IOS XR 64ビットソフトウェアの脆弱性が存在するリリースを実行し、インストールされているいずれかのラインカードに対して脆弱な設定が有効になっている次のシスコ製品に影響を与えます。

- ASR 9000シリーズアグリゲーションサービスルータ（LightspeedまたはLightspeed Plusベースのラインカードがインストールされている場合）
- ASR 9902 コンパクト高性能ルータ
- ASR 9903 コンパクト高性能ルータ

脆弱性が存在する Cisco 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。この脆弱性に対処する修正済みソフトウェアまたはSMUをインストールする前に、『ASR 9000シリーズルータのレイヤ3マルチキャストサービス拒否の脆弱性に対するCisco IOS XRソフトウェア』を参照してください。

取り付けられているラインカードの判別

デバイスにインストールされているラインカードを確認するには、show platform CLIコマンドを使用します。

Cisco ASR 9902 および 9903 コンパクト高性能ルータでは、Lightspeed-Plus ベースのラインカードが統合されます。

次のラインカードは Lightspeed ベースです。

- A9K-16X100GE-TR
- A99-16X100GE-X-SE
- A99-32X100GE-TR

次のラインカードは、Lightspeed Plus ベースです。

- A9K-4HG-FLEX-SE
- A9K-4HG-FLEX-TR
- A9K-8HG-FLEX-SE

- A9K-8HG-FLEX-TR
- A9K-20HG-FLEX-SE
- A9K-20HG-FLEX-TR
- A99-4HG-FLEX-SE
- A99-4HG-FLEX-TR
- A99-10X400GE-X-SE
- A99-10X400GE-X-TR
- A99-32X100GE-X-SE
- A99-32X100GE-X-TR

ラインカードのタイプの識別の詳細については、「ASR 9000シリーズラインカードタイプ」を参照してください。

注：Cisco Lightspeed-Plus製品IDのリストは、このドキュメントの発行時点で正確でした。製品 ID に関して具体的な質問がある、またはさらに詳しく知りたい場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

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

次の両方に該当する場合、デバイスは脆弱です。

- IPv4 ACLグループまたはQoSポリシーは、入力方向または出力方向で、レイヤ2、レイヤ3、またはブリッジ仮想インターフェイスに適用されます。
- IPv4 ACLグループまたはQoSポリシーは、LightspeedカードまたはLightspeed-Plusカードのいずれかに存在するインターフェイス上にあります。

次の例は、インターフェイスTenGigE0/0/0/0に適用されたサービスポリシーと、インターフェイスTenGigE0/0/0/1に適用されたIPv4アクセスグループを示しています。

<#root>

```
Router#
show running-config


interface TenGigE0/0/0/0
 .
 .
 service-policy input QoS_INGRESS
 service-policy output QoS_EGRESS
.
.
interface TenGigE0/0/0/1
.
.
 ipv4 access-group ACL_INGRESS ingress
 ipv4 access-group ACL_EGRESS egress
.
```

```
.

Router#
```

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
- 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ないIOS XRプラットフォーム
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。ただし、設定されているIPv4 ACLまたはQoSポリシーを該当するインターフェイスから削除することで、この脆弱性は緩和されます。

この緩和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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通

常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性に対処する修正済みソフトウェアまたはSMUをインストールする前に、『ASR 9000シリーズルータのレイヤ3マルチキャストサービス拒否の脆弱性に対するCisco IOS XRソフトウェア』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）
7.8 以前	修正済みリリースに移行。
7.9	7.9.21
7.10	7.10.2
7.11 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-ipv4uni-LfM3cfBu

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。