

# ASR 9000 シリーズ ルータ向け Cisco IOS XR ソフトウェアのレイヤ 3 マルチキャストにおけ るサービス妨害 ( DoS ) の脆弱性



アドバイザリーID : cisco-sa-multicast-  
ERMrSvq7

[CVE-2025-  
20146](#)

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 : [CSCwm45759](#)

[CSCwm63979](#)

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向け Cisco IOS XR ソフトウェアのレイヤ 3 マルチキャスト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、サービス妨害 ( DoS ) 状態が発生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 アクセス制御リスト ( 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した不正な形式の IPv4 マルチキャストパケットの不適切な処理に起因します。攻撃者は、巧妙に細工された IPv4 マルチキャストパケットを該当デバイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はラインカード例外やハードリセットを引き起こし、ラインカードのリロード中にラインカード上のトラフィックが失われ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。この脆弱性に対処するための軽減策があります。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multicast-ERMrSvq7>

このアドバイザリーは、2025 年 3 月に公開された Cisco IOS XR ソフトウェアリリースのセキュリティ アドバイザリー バンドルに含まれています。アドバイザリーとリンクの一覧については、[Cisco](#)

[Event Response: March 2025 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

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ており、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性のある設定が有効になっている以下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。

この脆弱性は、Cisco Bug ID [CSCwf56155](#) を修正したコードによって引き起こされました。その修正を含むソフトウェアリリースまたは SMU に脆弱性があります。詳細については、「[ASR 9000 シリーズ ルータ向け Cisco IOS XR ソフトウェアの IPv4 ユニキャストパケットにおけるサービス妨害 \( DoS \) の脆弱性](#)」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、公開時点で正確な内容です。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。

## デバイスの設定に脆弱性があるかどうかの確認

該当デバイスは、次の両方が当てはまる場合、脆弱な設定になっています。

- IPv4 ACL グループまたは QoS ポリシーが、Lightspeed または Lightspeed-Plus カード上に存在するインターフェイスに、入力方向または出力方向のいずれかで適用されている。
- デバイスがレイヤ 3 マルチキャストまたはマルチキャスト VPN ( MVPN ) で設定されている。

次に、レイヤ 3 マルチキャストで設定され、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 アクセスグループがあるデバイスの例を示します。

```
<#root>
```

```
Router#
```

```
show running-config multicast-routing
```

```
Wed Nov 13 00:08:58.920 UTC
```

```
multicast-routing
```

```
address-family ipv4
```

```
.
```

```
.
```

```
<output omitted>
```

```
<#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](#)」セクションにリストされていない 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、設定済みの IPv4 ACL または QoS ポリシーを該当インターフェイスから削除すると、この脆弱性は軽減されます。

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ン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です。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](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

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 )
7.9.2 以前	影響なし。
7.9.21	修正済みリリースに移行。
7.10.1	影響なし。
7.10.2	修正済みリリースに移行。
7.11	修正済みリリースに移行。
24.1	修正済みリリースに移行。
24.2	24.2.21 (future release)
24.3	修正済みリリースに移行。
24.4 以降	影響なし。

SMU もこの脆弱性に対処するために使用できます。記載されていないプラットフォームやリリース向けの 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。この脆弱性に関して公開されている可能性がある SMU の特定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-multicast-ERMrSvq7>

## 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

本アドバイザーは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザーの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 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。