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



Advisory ID : cisco-sa-asr9k-tUyxcyXN
初公開日 : 2026-10-21 16:00
バージョン 1.0 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco Bug ID : CSCwn39554

CVE-2026-76505

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco ASR 9000および9900シリーズアグリゲーションサービスルータ、Cisco ASR 9902および9903コンパクト高性能ルータに影響するCisco IOS XRソフトウェアのIPv4パケット処理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ネットワークプロセッサ(NP)エラーを引き起こし、その結果、ラインカードがリセットまたはシャットダウンされ、サービス妨害(DoS)状態になる可能性があります。

この脆弱性は、該当のラインカードインターフェイスで受信され、for-usトラフィックとして処理される巧妙に細工されたIPv4パケットの不適切な処理に起因します。この問題によりNPがリセットされ、回復中に該当ラインカードでトラフィック損失が発生する可能性があります。リセット状態が繰り返されると、ネットワークプロセッサが永続的なシャットダウン状態になる場合があります。その場合、トラフィックを復元するために、明示的なラインカードのリロードが必要になることがあります。

この脆弱性は、IPv4パケット処理パス内にあります。通過するIPv4トラフィックではこの問題は発生せず、IPv6トラフィックでは発生しません。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-asr9k-tUyxcyXN

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任意のラインカードのインターフェイスでIPv4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 9900 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。

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ASR 9903コンパクト高性能ルータは、Lightspeed-Plusベースのラインカードを統合しています。

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
- A9K-16X100GE-CM
- A99-32X100GE-CM

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
- A9K-20HG-FLEX-FC
- A9K-8HG-FLEX-FC
- A9K-4HG-FLEX-FC
- A99-4HG-FLEX-FC
- A99-32HG-FC
- A99-4T-FC

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のタイプについて」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

IPv4アドレスが設定されているデバイスは、脆弱であると見なされます。次の例は、IPv4が設定された単一のインターフェイスを持つデバイスを示しています。

<#root>

```
Router#
show ipv4 vrf all interface brief

Wed Oct 21 16:00:00.000 UTC
TenGigE0/0/0/12                198.51.100.1      Up              Up       default
Router#
```

IPv6のみの設定は、この脆弱性の影響を受けません。

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

- 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ソフトウェアプラットフォーム
- NX-OS ソフトウェア

詳細

ラインカードのリロードまたはエラーがこの状態によって発生したかどうかを判断するには、次の動作コマンドを使用して、NPのリセットを確認します。適切なサポート組織と協力して結果を確認します。

```
Router# show logging | include "NP.*reset"
```

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、緩和策があります。

この脆弱性を緩和するには、UDP宛先ポート1701を使用して、インフラストラクチャアドレス空間を宛先とするUDPトラフィックをフィルタリングします。

任意のエッジまたは外部インターフェイスに入力インフラストラクチャアクセスコントロールリスト(iACL)を設定し、トランジットトラフィックの転送を続行しながら、ローカルルータアドレス宛てのUDPポート1701トラフィックをドロップします。

既存のiACLステートメントに組み込む必要があるスニペットの例を次に示します。

```
ipv4 access-list ACL_INFRA_PROTECTION
 ! Permit required routing and management protocols
 permit ospf any any
 permit bgp any host <LOCAL_ROUTER_IP>
 permit icmp any any echo-reply
 !
 ! Deny UDP 1701 destined ONLY to router interface/loopback IPs
 deny udp any host <ROUTER_INTERFACE_IP> eq 1701
 deny udp any host <ROUTER_LOOPBACK_IP> eq 1701
 deny udp any <ROUTER_INFRA_SUBNET> <WILDCARD_MASK> eq 1701
 !
 ! Permit all customer transit traffic
 permit ipv4 any any
!
interface <interface-id>
 ipv4 access-group ACL_INFRA_PROTECTION ingress
```

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正リリース

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	第 1 修正済みリリース
7.8 以前	修正済みリリースに移行。
7.9	7.9.2およびSMU asr9k-x64-7.9.2.CSCwn39554 7.9.21およびSMU asr9k-x64-7.9.21.CSCwn39554
7.10	7.10.2およびSMU asr9k-x64-7.10.2.CSCwn39554
7.11	7.11.2およびSMU asr9k-x64-7.11.2.CSCwn39554 7.11.21およびSMU asr9k-x64-7.11.21.CSCwn39554
24.1	24.1.2およびSMU asr9k-x64-24.1.2.CSCwn39554
24.2	24.2.2およびSMU asr9k-x64-24.2.2.CSCwn39554 24.2.21
24.3	24.3.2およびSMU asr9k-x64-24.3.2.CSCwn39554
24.4	24.4.2
25.1 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。

注：これらのSMUはIn-Service Software Upgrade(ISSU)/Reload SMUのインストールの影響タイプです。

シスコの 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済み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。

送信元

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-asr9k-tUyxcyXN

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月21日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center（TAC）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。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。本アドバイザリ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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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済みリリース情報のみを評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。