Cisco IOS XRソフトウェアのレイヤ2サービスにおけるDoS脆弱性

アドバイザリーID : cisco-sa-xrl2vpn-jesrU3fc
初公開日 : 2024-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCwe29150

CVE-2024-20318

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ソフトウェアのレイヤ2イーサネットサービスにおける脆弱性により、認証されていない隣接する攻撃者がラインカードのネットワークプロセッサをリセットさせ、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、レイヤ2サービス機能が有効になっているラインカードで受信された特定のイーサネットフレーム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特定のイーサネットフレーム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、攻撃者は入力インターフェイスのネットワークプロセッサをリセットさせ、ネットワークプロセッサがサポートするインターフェイスを介したトラフィックを損失させる可能性があります。ネットワークプロセッサを何度もリセットすると、ラインカードがリセットされ、DoS状態が発生します。

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-xrl2vpn-jesrU3fc

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

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、該当するレイヤ2トランスポート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。

- LightspeedベースまたはLightspeed Plusベースのラインカードがインストールされた 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
- ASR 9903 コンパクト高性能ルータ
- IOS XRd vRouter
- IOS XRv 9000 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確認

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。

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のタイプ

について」を参照してください。

注：このドキュメントの発行時点では、Cisco LightspeedおよびLightspeed-Plus製品ID(PID)のリストは正確でした。PIDに関する具体的な質問や詳細説明については、Cisco Technical Assistance Center(TAC)にお問い合わせください。

レイヤ2トランスポート設定の決定

デバイスに該当するレイヤ2トランスポート設定があるかどうかを確認するには、次の手順を実行します。

1. show running-configurationコマンドを使用します。
2. 次の例に示すように、出力のl2transportインターフェイスでrewrite ingress tag popを探します。
   <#root>

```
!
interface HundredGigE0/0/0/12.1 l2transport
 encapsulation dot1q 2500


rewrite ingress tag pop 1 symmetric


!
```

   rewrite ingress tag popが出力に表示されない場合、そのデバイスには脆弱性はありません。

3. rewrite ingress tag popが出力に表示される場合は、デバイスに次のいずれかが存在するかどうかを確認します。
   - ロードバランシングフロー**src-dst-ip**は、次の例に示すように、l2vpn設定の下に存在します。
     <#root>

```
l2vpn
router-id 1.1.1.1

load-balancing flow src-dst-ip
```

   - IPヘッダーを調べるサービスポリシーまたはアクセスコントロールフィルタリングメカニズムは、レイヤ2インターフェイスに適用されます。

   設定またはポリシーのいずれかがデバイスに存在する場合、そのデバイスには脆弱性が存在します。

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。

緩和策として、load-balancing flow src-dst-ipが設定されている場合はこれを削除するか、IPヘッダーを検査しないようにサービスポリシーを変更します。

これら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。

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

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

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	7.9.2
7.10	7.10.1

シスコはこの脆弱性に対処する次の SMU もリリースしています。

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。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.3.2	ASR9K-X64	asr9k-x64-7.3.2.CSCwe29150
7.4.2	ASR9K-X64	asr9k-x64-7.4.2.CSCwe29150
7.5.2	ASR9K-X64	asr9k-x64-7.5.2.CSCwe29150
7.7.2	ASR9K-X64	asr9k-x64-7.7.2.CSCwe29150
7.8.2	ASR9K-X64 XRD-VROUTER	asr9k-x64-7.8.2.CSCwe29150 xrd-vrouter-7.8.2.CSCwe29150

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-xrl2vpn-jesrU3fc

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。