Cisco IOS XR ソフトウェアの IPv6 フラッドにおけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-xripv6-spJem78K

初公開日 : 2021-02-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : Yes

Cisco バグ ID : CSCvv45504

CVE-2021-1268

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ソフトウェアの管理インターフェイスのIPv6プロトコル処理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、該当デバイスの管理インターフェイスネットワークでIPv6フラッドを発生させる可能性があります。

この脆弱性は、ソフトウェアがIPv6ノードローカルマルチキャストグループアドレスの宛先を持ち、管理インターフェイスで受信されたIPv6パケットを誤って転送するために存在します。攻撃者は、管理インターフェイスと同じネットワークに接続し、IPv6ノードローカルマルチキャストグループアドレスの宛先を持つIPv6パケットを注入することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は対応するネットワークでIPv6フラッドを引き起こす可能性があります。そのネットワークセグメント上のCisco IOS XRソフトウェアノードの数に応じて、不正利用によりネットワークトラフィックが過剰に発生し、その結果、ネットワークの低下やサービス拒否(DoS)状態が発生す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ました。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XRソフトウェアの脆弱性のあるリリースを実行し、管理インターフェイスが次の両方で設定されているシスコデバイスに影響を与えます。

- IPv6アドレス
- 管理インターフェイスセグメントでネクストホップを使用するデフォルトのIPv6スタティックルート

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。

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。

詳細

この脆弱性がエクスプロイトされた場合、ネットワークに転送されるパケットの数は、ネットワークセグメントに接続されている Cisco IOS XR ソフトウェア管理インターフェイスの数によって決まります。管理インターフェイスがあり、同じレイヤ 2 ドメインに接続されている Cisco IOS XR デバイスが多いほど、レイヤ 2 セグメントで転送されるパケットが多くなります。転送されるパケットの数が多すぎると、ネットワークパフォーマンスが低下し、ネットワーク上でサービス妨害（DoS）状態が発生する可能性があります。

回避策

デフォルトの IPv6 スタティックルートを削除し、プレフィックス固有のルートを追加すると、この脆弱性が緩和されます。たとえば、デフォルトのIPv6スタティックルートを削除し、2000::/3 <ネクストホップ>のIPv6スタティックルートを追加すると、この脆弱性が緩和されます。

修正済みソフトウェア

シスコでは、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 アップデートを提供しています。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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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

ユリティ 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。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この脆弱性は、Cisco IOS XR ソフトウェアリリース 6.7.3、7.1.3、7.2.2、7.3.1 で修正されています。

シスコは、この脆弱性に対処するためのソフトウェア メンテナンス アップグレード（SMU）をリリースしました。他のプラットフォームおよびリリースに 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	プラットフォーム	SMU 名
6.3.1	NCS1K	ncs1k-6.3.1.CSCvv45504
	NCS1001	ncs1001-6.3.1.CSCvv45504
6.5.2	NCS1K	ncs1k-6.5.2.CSCvv45504
	NCS1001	ncs1001-6.5.2.CSCvv45504

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2021 年 2 月 3 日

利用規約