Cisco IOS XRソフトウェアのNetwork Convergence SystemにおけるDenial of Service(DoS)の脆弱性

アドバイザリーID : cisco-sa-l2services-2mvHdNuC
初公開日 : 2024-09-11 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 : CSCwh30122

CVE-2024-20317

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

さまざまなCisco Network Convergence System(NCS)プラットフォームに対するCisco IOS XRソフトウェアによる特定のイーサネットフレームの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重要な優先パケットをドロップさせ、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、インターフェイスで受信される特定のタイプのイーサネットフレームの誤った分類に起因します。攻撃者は、該当デバイスとの間で特定のタイプのイーサネットフレームを送受信することにより、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、コントロールプレーンプロトコルの関係でエラーが発生し、DoS状態に陥る危険性があります。詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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-l2services-2mvHdNuC

このアドバイザリは、2024年9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: September 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ソフトウェアの脆弱性が存在するリリースを実行し、レイヤ2イーサネットサービスが設定されている次のCisco NCSデバイスに影響を与えます。

- NCS 55A1固定シャーシ
- NCS 55A2固定シャーシ
- NCS 540シリーズルータ（N540-24Q8L2DD-SYSを除く）
- NCS 560 シリーズ ルータ
- NCS 5500シリーズモジュラシャーシ[1]
- NCS 5501固定シャーシ
- NCS 5502固定シャーシ

1. NCS57以降を除くすべての製品IDがこの脆弱性の影響を受けます。詳細については、『Cisco Network Convergence System 5500シリーズモジュラシャーシ』のデータシートを参照してください。

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。

デバイスにレイヤ2イーサネットサービスが設定されているかどうかを確認する

デバイスでレイヤ2サービスが設定されているかどうかを確認するには、show running-configコマンドを使用します。 | include l2transportコマンドを使用します。出力が返された場合、デバイスは次の例のように影響を受けます。

<#root>

```
RP/0/RP0/CPU0:NCS5501#show running-config | include l2transport

Tue Jan 16 01:14:07.977 UTC
Building configuration...
interface GigabitEthernet0/0/0/1.200 l2transport

RP/0/RP0/CPU0:NCS5501#
```

出力から情報が返されない場合、デバイス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

詳細

レイヤ2インターフェイスで特定のフレームが受信されると、それらは誤ってトラフィッククラス7仮想出力キュー(TC7 VOQ)に分類されます。維持されたレートでこれらのフレームが十分に送信されると、VOQはTC7でパケットのドロップを開始します。影響を受けるポートは、レイヤ2トラフィックがデバイスからの出力を受信するインターフェイスです。ほとんどの場合、これはサービスプロバイダーのコアインターフェイスです。

コントロールプレーントラフィックもこのキュー内で処理されるため、この脆弱性が原因でキープアライブまたはhelloパケットがドロップされ、OSPF、Intermediate System-to-Intermediate System(ISIS)、双方向フォワーディング検出(BFD)、ボーダーゲートウェイプロトコル(BGP)、およびラベル配布プロトコル(LDP)などのプロトコルでDoS状態が発生する可能性があります。

VOQの状態をモニタするには、show controllers npu stats voq ingress interfaceコマンドを使用します。次の例は、使い果たしたTC_7 VOQのコマンド出力を示しています。

<#root>

```
RP/0/RP0/CPU0:NCS-5501#
```

show controllers npu stats voq ingress interface tenGigE 0/0/0/2 instance 0 location 0/0/CPU0

```
Wed Mar 13 16:00:00.000 UTC
Interface Name    =    Te0/0/0/2
Interface Handle  =          118
Location          =     0/0/CPU0
Asic Instance     =            0
VOQ Base          =         1088
Port Speed(kbps)  =     10000000
Local Port        =        local
       ReceivedPkts    ReceivedBytes   DroppedPkts     DroppedBytes
-----------------------------------------------------------------
Core-0:
TC_0 = 0              0               0               0
TC_1 = 47708616       37410160369     0               0
TC_2 = 0              0               0               0
TC_3 = 0              0               0               0
TC_4 = 0              0               0               0
TC_5 = 0              0               0               0
TC_6 = 0              0               0               0
```

```
TC_7 = 11033161168     1108832775990   6905125762      791656829609


Core-1:
TC_0 = 0               0               0               0
TC_1 = 0               0               0               0
TC_2 = 0               0               0               0
RP/0/RP0/CPU0:NCS-5501#
```

回避策

この脆弱性に対処する回避策はありません。

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またはトレインを示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された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）
7.6 以前	影響なし。
7.7	修正済みリリースに移行。
7.8	修正済みリリースに移行。
7.9	修正済みリリースに移行。
7.10	7.10.2
7.11	7.11.1
24.1	24.1.1

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。次の表に記載されていないリリースで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。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.8.2	NCS540	ncs540-7.8.2.CSCwh30122
7.9.2	IOSXRWBD NCS5500	iosxrwbd-7.9.2.CSCwh30122 ncs5500-7.9.2.CSCwh30122

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-l2services-2mvHdNuC

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9月11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。