ASR 9000 シリーズ ルータ向け Cisco IOS XR ソフトウェアの Bidirectional Forwarding Detection におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-bfd-XmRescbT

初公開日 : 2023-03-08 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : Yes

Cisco バグ ID : CSCwc39336

CVE-2023-20049

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ソフトウェアの双方向フォワーディング検出(BFD)ハードウェアオフロード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、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、BFDハードウェアオフロード機能が有効になっているラインカードで受信される不正なBFD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 BFD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、攻撃者はラインカードの例外またはハードリセットを引き起こし、その結果、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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT

このアドバイザリは、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公開の2023年3月リリースの一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco

Event Response: March 2023 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 BFD ハードウェアオフロード機能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のみ）
- 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

デバイスに取り付けら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 リストの製品 ID 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。

BFD ハードウェアオフロードが有効になっているかどうかの確認

BFD ハードウェアオフロードが有効になっているラインカードを確認するには、**show bfd hw-offload state** CLI コマンドを使用します。前述のラインカードのいずれかで構成および動作状態が有効になっている場合、デバイスはこの脆弱性の影響を受けます。次の例は、BFD ハードウェアオフロードが有効になっていないデバイスを示しています。

```
RP/0/RSP0/CPU0:ASR9006#show bfd hw-offload state Wed Mar 8 16:00:00.000 UTC BFD HW OFFLOAD Feature
state: 0/2/CPU0 ----------------- Configuration State: Disabled Operational State: Disabled
RP/0/RSP0/CPU0:ASR9006#
```

次の例は、BFD ハードウェアオフロードが有効になっているデバイスを示しています。

```
RP/0/RSP0/CPU0:ASR9006#show bfd hw-offload state Wed Mar 8 16:00:00.000 UTC BFD HW OFFLOAD Feature
state: 0/2/CPU0 ----------------- Configuration State: Enabled
Operational   State:  Enabled
RP/0/RSP0/CPU0:ASR9006#
```

BFD ハードウェアオフロードが有効になっている場合でも、すべての BFD セッションがハードウェアで処理されるわけではありません。次の例に示すように、少なくとも 1 つの BFD セッションの [H/W] が [はい] と表示されている必要があります。

```
RP/0/RSP0/CPU0:ASR9006#show bfd all session Wed Mar 8 16:00:00.000 UTC IPv4: ----- Interface Dest Addr Local
det time(int*mult) State
Echo Async H/W NPU ---------- ------------- ------------ ---------------- ---------- ti100 10.0.0.1 0s(0s*0)
900ms(300ms*3) UP
No     n/a
Hu0/2/0/15 192.168.100.100 0s(0s*0) 900ms(300ms*3) UP
Yes    0/2/CPU0
RP/0/RSP0/CPU0:ASR9006#
```

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

この脆弱性は、IPv6 BFD パケットではエクスプロイトできません。ただし、IPv6 BFD セッションでも接続されたインターフェイスに IPv4 アドレスが設定されている場合、攻撃者は、インターフェイスに設定された IPv4 アドレスに細工された IPv4 BFD パケットを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。インターフェイス Te0/1/0/10/0 にも IPv4 アドレス 192.168.1.1 が設定されている場合、次の例に示すように、攻撃者は 192.168.1.1 に細工された IPv4 BFD パケットを送信することにより、IPv6 BFD セッションをエクスプロイトする可能性があります。

```
RP/0/RSP0/CPU0:ASR9006#show bfd all session Wed Mar 8 16:00:00.000 UT IPv4: ----- IPv6: ----- Interface
Dest Addr Local det time(int*mult) State H/W NPU Echo Async ------------------- --------------- -----------
----- ---------------- ---------- Te0/1/0/10/0 fe80::36f8:e7ff:fee0:947 Yes 0/1/CPU0 0s(0s*0)
900ms(300ms*3) UP
```

回避策

この脆弱性に対処する回避策と軽減策があります。

この脆弱性を完全に軽減する唯一の回避策は、BFD ハードウェアオフロードを無効にすることです。インフラストラクチャ アクセス制御リスト（iACL）の作成は、攻撃対象領域のみを制限する軽減策です。

BFD ハードウェアオフロードの無効化

BFD ハードウェアオフロードを無効にするには、次の例に示すように、**hw-module bfw-hw-offload enable** コマンドをすべて削除し、割り当てられたラインカードをリセットします。

```
RP/0/RSP0/CPU0:ASR9006#config terminal
Wed Mar 8 16:00:00.000 UTC
RP/0/RSP0/CPU0:ASR9006(config)#no hw-module bfd-hw-offload enable location 0/2/CPU0
RP/0/RSP0/CPU0:ASR9006(config)#commit
RP/0/RSP0/CPU0:ASR9006(config)#end
RP/0/RSP0/CPU0:ASR9006#hw-module subslot 0/2/CPU0 reload
```

インフラストラクチャ アクセス制御リストの作成

iACL では攻撃対象領域は制限されますが、許可されたピアからのエクスプロイトは防止されず、スプーフィングの対象となります。

次の例は、インフラストラクチャ BFD ピアのみを許可する iACL を示しています（192.0.2.x/24 はインフラストラクチャ アドレス空間です）。

```
RP/0/RSP0/CPU0:ASR9006# show running-config ipv4 access-list
ipv4 access-list BFD_DROP
5 remark * Mark sure to Allow Legitimate BFD peers *
 10 permit udp 192.0.2.0 0.0.0.255 192.0.2.0 0.0.0.255 eq bfd
11 remark * Depending on BFD deployment may need *
12 permit udp 192.0.2.0 0.0.0.255 192.0.2.0 0.0.0.255 eq 4784
 13 permit udp 192.0.2.0 0.0.0.255 192.0.2.0 0.0.0.255 eq 6784
15 remark * Drop all other attempts to the infrastructure address space *
 20 deny udp any 192.0.2.0 0.0.0.255 eq bfd
 30 permit ipv4 any any
!
RP/0/RSP0/CPU0:ASR9006#
```

この iACL をすべての公開インターフェイスに適用します。

次の例は、存続可能時間（TTL）が 255（シングルホップセッション用に想定）の BFD パケットのみを許可する iACL を示しています。

```
RP/0/RSP0/CPU0:ASR9006# show running-config ipv4 access-list
ipv4 access-list BFD_DROP_TTL
5 remark * Drop based purely on TTL. Allow our Single Hop BFD sessions *
10 permit udp any 192.0.2.0 0.0.0.255 eq bfd ttl eq 255
11 remark * Depending on BFD deployment may need *
12 permit udp any 192.0.2.0 0.0.0.255 eq 4784 ttl eq 255
13 permit udp any 192.0.2.0 0.0.0.255 eq 6784 ttl eq 255
14 remark * You would need to tune the above two lines for multi-hop sessions *
15 remark * Deny anything else for BFD *
20 deny udp any any eq bfd ttl lt 255
21 remark * You would need to tune the above line for multi-hop sessions *
30 permit ipv4 any any
!
RP/0/RSP0/CPU0:ASR9006#
```

この iACL をすべての公開インターフェイスに適用します。

この回避策と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 Cisco Support and Downloads 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）
6.5	修正済みリリースに移行。
6.6	修正済みリリースに移行。
7.0	修正済みリリースに移行。
7.1	修正済みリリースに移行。
7.3	修正済みリリースに移行。
7.4	修正済みリリースに移行。
7.5	7.5.3
7.6	7.6.2
7.7 以降	7.7.1

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
7.1.3	ASR9K-X64	asr9k-x64-7.1.3.CSCwc39336
7.3.2	ASR9K-X64	asr9k-x64-7.3.2.CSCwc39336
7.5.2	ASR9K-X64	asr9k-x64-7.5.2.CSCwc39336

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-bfd-XmRescbT

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	2023 年 3 月 8 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。