ASR 9000シリーズアグリゲーションサービスルータ用Cisco IOS XRソフトウェアのPPPoEにおけるDoS脆弱性

アドバイザリーID : cisco-sa-iosxr-pppma-JKWFgneW
CVE-2024-20327
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 : CSCwf75789

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用Cisco IOS XRソフトウェアのPPP over Ethernet(PPPoE)終端機能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ppp_maプロセスをクラッシュさせ、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、LightspeedベースまたはLightspeed-Plusベースのラインカード上でPPPoE終端を使用するブロードバンドネットワークゲートウェイ(BNG)機能を実行しているルータで受信される不正なPPPoEパケットの不適切な処理に起因します。攻撃者は、PPPoEを終了しない該当のラインカードインターフェイスに、巧妙に細工されたPPPoEパケットを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はppp_maプロセスをクラッシュさせ、その結果、ルータ全体でPPPoEトラフィックの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-iosxr-pppma-JKWFgneW

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ソフトウェアの脆弱性が存在するリリースを実行し、次の特性をすべて備えたCisco ASR 9000シリーズアグリゲーションサービスルータに影響を与えます。

- インストールされているLightspeedベースまたはLightspeed Plusベースのラインカード
- PPPoE終端が有効なBNG
- 影響を受けるラインカード上でPPPoEが有効になっているインターフェイスまたはサブインターフェイスが少なくとも1つ
- PPPoEが有効になっていないインターフェイスまたはサブインターフェイスが、該当するラインカード上に1つ以上ある

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。

次の例は、2枚のLightspeed A99-32X100GE-X-SEラインカードとLightspeed-Plus A99-4HG-FLEX-TRラインカードがインストールされているデバイスの出力を示しています。

<#root>

```
RP/0/RSP1/CPU0:ASR-9906-D#show platform
Thu Feb 1 20:18:56.754 UTC
Node               Type                       State            Config state
--------------------------------------------------------------------------------
0/RSP0/CPU0        A9K-RSP5-SE(Standby)       IOS XR RUN       NSHUT
0/RSP1/CPU0        A9K-RSP5-SE(Active)        IOS XR RUN       NSHUT
0/FT0              ASR-9906-FAN               OPERATIONAL      NSHUT
0/FT1              ASR-9906-FAN               OPERATIONAL      NSHUT
0/0/CPU0           A99-32X100GE-X-SE          IOS XR RUN       NSHUT
0/1/CPU0           A99-32X100GE-X-SE          IOS XR RUN       NSHUT
0/2/CPU0           A9K-48X10GE-1G-SE          IOS XR RUN       NSHUT
0/3/CPU0           A99-4HG-FLEX-TR            IOS XR RUN       NSHUT
0/FC0              A99-SFC3-T                 OPERATIONAL      NSHUT
```

```
0/FC1              A99-SFC3-T                 OPERATIONAL       NSHUT
0/FC2              A99-SFC3-T                 OPERATIONAL       NSHUT
0/FC4              A99-SFC3-T                 OPERATIONAL       NSHUT
0/PT0              A9K-AC-PEM-V3              OPERATIONAL       NSHUT
RP/0/RSP1/CPU0:ASR-9906-D#
```

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-TR
- A9K-4HG-FLEX-SE
- A99-4HG-FLEX-TR
- A99-4HG-FLEX-SE
- A9K-8HG-FLEX-TR
- A9K-8HG-FLEX-SE
- A9K-20HG-FLEX-TR
- A9K-20HG-FLEX-SE
- A99-32X100GE-X-TR
- A99-32X100GE-X-SE
- A99-10X400GE-X-TR
- A99-10X400GE-X-SE

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。

BNG PPPoEがグローバルに有効になっているかどうかの確認

BNG PPPoEがグローバルに有効になっているかどうかを確認するには、show running-config pppoe bba-groupコマンドを使用します。次の例に示すように、ブロードバンドアグリゲーション(BBA)グループにpppoe bba-groupが含まれている場合は、BNG PPPoEが有効になっています。

<#root>

```
RP/0/RSP1/CPU0:ASR-9906-D#show running-config pppoe bba-group
Thu Feb 1 21:19:21.003 UTC
```

```
pppoe bba-group

TS-PPPOE
 service selection disable
 sessions max limit 32000
!
RP/0/RSP1/CPU0:ASR-9906-D#
```

インターフェイスでBNG PPPoEが有効になっているかどうかの確認

インターフェイスでBNG PPPoEが有効になっているかどうかを確認するには、show running-config interface | utility egrep "interface|pppoe enable bba-group|bundle id"コマンドを発行します。インターフェイスまたはサブインターフェイスでpppoe enable bba-groupが設定されている場合、BNG PPoEが有効になります。

次の例は、次の特性を持つデバイスの出力を示しています。

- インターフェイスBundle-Ether41.50ではPPPoEが有効になっています。
- インターフェイスTenGigE0/3/0/0はバンドルEther41の一部として設定されています。
- インターフェイスTenGigE0/3/0/0は、Lightspeed-PlusベースのラインカードA99-4HG-FLEX-TR上にあり、PPPoEが有効になっています。

<#root>

```
RP/0/RSP1/CPU0:ASR-9906-D#show running-config interface | utility egrep "interface|pppoe enable bba-g
Thu Feb 1 22:12:42.769 UTC
interface Bundle-Ether20
interface Bundle-Ether20
interface Bundle-Ether41

interface Bundle-Ether41.50


 pppoe enable bba-group TS-PPPOE


interface Bundle-Ether41.55
interface Loopback0

interface TenGigE0/3/0/0


 bundle id 41 mode on


.
.
.
```

注：分かりやすくするために、上記の出力は、表示するインターフェイスが少なくなるように

変更されています。

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
- 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。

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	7.9.21
7.10	7.10.1
7.11	7.11.1

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
7.5.2	ASR9K-X64	asr9k-x64-7.5.2.CSCwf75789

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-iosxr-pppma-JKWFgneW

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。