Cisco IOS XRソフトウェアのIPv6における不正なパケットによるDoS脆弱性

High

アドバイザリーID : cisco-sa-20140611-ipv6 CVE-2014-2176
初公開日 : 2014-06-11 16:00
最終更新日 : 2014-06-13 14:01
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCun71928

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

ASR 9000シリーズアグリゲーションサービスルータ用のCisco IOS XRソフトウェアにおける不正なInternet Protocol version 6(IPv6)パケットの解析における脆弱性により、認証されていないリモートの攻撃者が、ネットワークプロセッサ(NP)チップのロックアップと、最終的にトラフィックを処理するラインカードのリロードを引き起こす可能性があります。この脆弱性の影響を受けるのは、Cisco ASR 9000シリーズアグリゲーションサービスルータのTridentベースのラインカードのみです。

この脆弱性は、不正なIPv6パケットを解析する際の不十分なロジックに起因します。攻撃者は、不正なIPv6パケットのストリームを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はNPチップとラインカードのロックアップと最終的なリロードを引き起こし、サービス妨害(DoS)状態を引き起こす可能性があります。

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-20140611-ipv6

該当製品

脆弱性のある製品

Tridentベースのラインカードを搭載したCisco ASR 9000シリーズルータは、この脆弱性の影響を受けます。この脆弱性の影響を受けるためには、デバイスでIPv6を設定する必要はありません。

第1世代のCisco ASR 9000シリーズイーサネットラインカードは、Tridentベースのラインカードと呼ばれます。この呼び方は、これらのラインカードに使用されている NP に由来します。

次のラインカードはTridentベースです。

- A9K-40GE-L
- A9K-40GE-B
- A9K-40GE-E
- A9K-4T-L
- A9K-4T-B
- A9K-4T-E
- A9K-8T/4-L
- A9K-8T/4-B
- A9K-8T/4-E
- A9K-2T20GE-L
- A9K-2T20GE-B
- A9K-2T20GE-E
- A9K-8T-L
- A9K-8T-B
- A9K-8T-E
- A9K-16T/8-B

ASR 9000シリーズルータのラインカードがTridentベースかどうかを確認するには、 show diagコマンドを使用します。該当するデバイスには、少なくとも1つのTridentベースカードのPIDが含まれます。次の例は、A9K-40GE-Bカードがアクティブになっているデバイスを示しています。

<#root>

```
RP/0/RSP0/CPU0:router(admin)# show diag

Mon Jun 22 12:55:10.554 PST

NODE module 0/RSP0/CPU0 :
```

```
  MAIN:  board type 0x100302

!--- output truncated

NODE module 0/1/CPU0 :

   MAIN:  board type 0x20207
  S/N:   FOC123081J6
  Top Assy. Number:   68-3182-03


PID:   A9K-40GE-B


  UDI_VID:   V1D
  HwRev: V0.0
  New Deviation Number: 0
  CLEI:
  Board State : IOS XR RUN
  PLD:    Motherboard: N/A, Processor: 0x8004 (rev: 2.2), Power: N/A
  ROMMON: Version 1.0(20081208:174521) [ASR9K ROMMON]

!--- output truncated
```

脆弱性を含んでいないことが確認された製品

Typhoonベースのラインカードを搭載したCisco ASR 9000シリーズルータは、この脆弱性の影響を受けません。
ASR 9000シリーズイーサネットラインカードの第2世代は、Typhoonベースのラインカードと呼ばれることがよくあります。

次のラインカードはTyphoonベースです。

- A9K-MOD80-SE
- A9K-MOD80-TR
- A9K-MOD160-SE
- A9K-MOD160-TR

- A9K-24X10GE-SE
- A9K-24X10GE-TR
- A9K-36X10GE-SE
- A9K-36X10GE-TR
- A9K-2X100GE-SE
- A9K-2X100GE-TR
- A9K-1X100GE-SE
- A9K-1X100GE-TR

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

ASR 9000シリーズアグリゲーションサービスルータ用のCisco IOS XRソフトウェアにおける不正なInternet Protocol version 6(IPv6)パケットの解析における脆弱性により、認証されていないリモートの攻撃者が、ネットワークプロセッサ(NP)チップのロックアップと、最終的にトラフィックを処理するラインカードのリロードを引き起こす可能性があります。この脆弱性の影響を受けるのは、Cisco ASR 9000シリーズアグリゲーションサービスルータのTridentベースのラインカードのみです。

この脆弱性は、不正なIPv6パケットを解析する際の不十分なロジックに起因します。攻撃者は、不正なIPv6パケットのストリームを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はNPチップとラインカードのロックアップと最終的なリロードを引き起こし、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性が繰り返し悪用されると、長時間にわたってDoS状態が発生する可能性があります。

IPv6機能がこの脆弱性の影響を受けるようにするには、デバイスを設定する必要はありません。Tridentベースのラインカード上のインターフェイスでIPv6機能が有効になっていない場合、攻撃者は隣接ホストから不正なトラフィックを送信することしかできません。デバイスでIPv6機能が有効になっている場合、脆弱性はリモートネットワークから不正利用される可能性があります。

一部の中継装置では不正なIPv6パケットがブロックされる可能性がありますが、リモートネットワークから不正なパケットが発信され、該当デバイスでこの脆弱性が不正利用される可能性は依然として存在します。

この脆弱性は、Cisco Bug ID CSCun71928(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)CVE-2014-2176が割り当てられています。

回避策

この脆弱性に対する回避策はありません。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、次のリンク先にある付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco IOS XR Software IPv6 Malformed Packet Denial of Service Vulnerability』で参照できます。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=33986

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性と完全なアップグレード ソリューション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。

この脆弱性は、次のCisco IOS XRソフトウェアSMUで修正されています。

- asr9k-p-4.1.2.CSCun71928（バージョン4.1.2用）
- asr9k-p-4.2.1.CSCun71928およびasr9k-px-4.2.1.CSCun71928（バージョン4.2.1）
- asr9k-px-4.2.3.CSCun71928およびasr9k-p-4.2.3.CSCun71928（バージョン4.2.3）
- asr9k-px-4.3.1.CSCun71928（バージョン4.3.1用）
- asr9k-px-4.3.2.CSCun71928（バージョン4.3.2用）
- asr9k-px-4.3.4.CSCuo22306（バージョン4.3.4用）
- asr9k-px-5.1.1.CSCuo22306（バージョン5.1.1用）

Cisco IOS XRソフトウェアリリース5.1.2は、この脆弱性の影響を受けません。

注：追加バージョンのCisco IOS XRソフトウェアSMUは、利用可能になった時点で公開されます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

この脆弱性は、お客様のケースの調査中にCisco TACによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140611-ipv6

改訂履歴

リビジョン 1.1	2014年 6月13日	「ソフトウェアバージョンと修正」セクションに4.1.2ベースのSMUに関する情報を追加。
リビジョン 1.0	2014年 6月11日	初回公開リリース

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。