Cisco 集約はルータ 9000 シリーズ IPv6 フラグメント ヘッダ サービス拒否の脆弱性を保守します

High

アドバイザリーID : cisco-sa-20180131-ipv6

初公開日 : 2018-01-31 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvg46800

CVE-2018-0136

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 集約サービス ルータ（ASR）9000 シリーズ用の Cisco IOS XR ソフトウェア リリース 5.3.4 の IPv6 サブシステムの脆弱性は誘発するように非認証が、リモート攻撃者 サービス拒否（DoS）状態に終って 1つ以上の Trident ベースのラインカードのリロードをする、可能性があります。

脆弱性はフラグメント ヘッダ拡張の IPv6 パケットの不正確な処理が原因です。 攻撃者は設計されている IPv6 パケットの送信によって Trident ベースのラインカードにまたはを通して問題を誘発するようにこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者がラインカードが再起動するために奪取 する ある一定の時間の間に DoS に終って Trident ベースのラインカードのリロードを、誘発することを可能にする可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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。
131-ipv6

該当製品

脆弱性のある製品

この脆弱性は次の条件が満たされるとき Cisco 集約サービス ルータ（ASR）9000 シリーズに

影響を与えます:

- ルータは Cisco IOS XR ソフトウェア リリース 5.3.4 を実行しています。
- ルータは設定される IPv6 がある Trident ベースのラインカードをインストールしました。

Cisco IOS XR ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XR ソフトウェア リリースとそれを実行しているデバイスの名前は、管理者がデバイスにログインして、CLI で **show version** コマンドを使用することにより確認できます。 デバイスが Cisco IOS XR ソフトウェアを実行している場合、システム バナーに「 *Cisco IOS XR Software* 」などのテキストが表示されます。 デバイスで現在実行しているシステム イメージ ファイルの場所と名前は、「 *System image file is*」の横に表示されます。 ハードウェア製品の名前はシステム イメージ ファイル名の次の行に表示されます。

次の例は Cisco IOS XR ソフトウェア リリース 5.3.4 を実行しているデバイスの **show version コマンド**の出力を示したものです:

```
RP/0/RSP0/CPU0:ASR9001#show version
Wed Jan 24 01:32:32.751 EST

Cisco IOS XR Software, Version 5.3.4[Default]
Copyright (c) 2017 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 2.04(20140227:092320) [ASR9K ROMMON],

ASR9001 uptime is 6 hours, 17 minutes
System image file is "bootflash:disk0/asr9k-os-mbi-5.3.4.sp4-1.0.0/0x100000/mbiasr9k-rp.vm"

cisco ASR9K Series (P4040) processor with 8388608K bytes of memory.
P4040 processor at 1500MHz, Revision 2.0
ASR-9001 Chassis

2 Management Ethernet
8 TenGigE
20 GigabitEthernet
8 DWDM controller(s)
8 WANPHY controller(s)
44 GigabitEthernet/IEEE 802.3 interface(s)
219k bytes of non-volatile configuration memory.
2880M bytes of hard disk.
3932144k bytes of disk0: (Sector size 512 bytes).

Configuration register on node 0/RSP0/CPU0 is 0x2102
```

デバイスが Trident ベースのラインカードを備えていたかどうか確認します

Cisco ASR 9000 シリーズ イーサネット ラインカードの第 1 世代は、通常 Trident ベース (または *イーサネット*) ラインカードと呼ばれます。 この用語は、これらのラインカードで使用されるネットワーク プロセッサ (NP) に由来します。 以下は影響を受けた Trident ベースの

ラインカードの完全なリストです。 リストされていないラインカードはこの脆弱性から影響を受けません:

- 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-16/8T-B

ASR 9000 シリーズ ルータにインストールされるラインカードが Trident ベースであるかどうか判別するために、管理者は **show diag を**使用できます **| PID を含んで下さい:** コマンドを発行します。 影響を受けたデバイスは以前にリストされている Trident ベースのラインカードの少なくとも 1 つのためのプロダクト ID （ PID ）が含まれています。 次の例は A9K-8T-L カードがアクティブであるデバイスを示したものです:

```
RP/0/RSP0/CPU0:ASR9006-B#show diag | include PID:
Tue Jan 26 00:07:09.406 EST
  PID:    A9K-RSP440-SE
  PID:    A9K-RSP440-SE
  PID:    A9K-8X100GE-SE
  PID:    A9K-8T-L
  PID:    A9K-36X10GE-SE
  PID:    A9K-MOD160-TR
  PID:    A9K-MPA-8X10GE
  PID:    A9K-MPA-8X10GE
RP/0/RSP0/CPU0:ASR9006-B#
```

Trident ベースのラインカードに関する詳細については、次の URL で ASR 9000 シリーズ ラインカード タイプ出版物を参照して下さい: https://www.cisco.com/c/en/us/support/docs/routers/asr-9000-series-aggregation-services-routers/116726-qanda-product-00.html

デバイスが IPv6 のために設定されたかどうか確認します

管理者はインターフェイスが IPv6 トラフィック処理のためにイネーブルになっていたかどうか確認する **show ipv6 interface brief** コマンドを使用できます。 次の例は IPv6 処理のために設定されるインターフェイスを示したものです:

```
RP/0/RSP0/CPU0:ASR9006-B#show diag | include PID:
Tue Jan 26 00:07:09.406 EST
  PID:   A9K-RSP440-SE
  PID:   A9K-RSP440-SE
  PID:   A9K-8X100GE-SE
  PID:   A9K-8T-L
  PID:   A9K-36X10GE-SE
  PID:   A9K-MOD160-TR
  PID:   A9K-MPA-8X10GE
  PID:   A9K-MPA-8X10GE
RP/0/RSP0/CPU0:ASR9006-B#
```

show ipv6 interface brief コマンドは Cisco IOS XR ソフトウェアの実行バージョンが IPv6 をサポートしない場合エラーメッセージを表示します。 出力は IPv6 が無効である場合 IPv6 アドレスのインターフェイスを示さないものです。

インターフェイスは処理する IPv6 のためにインターフェイスがバンドルまたはバーチャルルーティングおよび転送（VRF）例の一部である場合設定されるかもしれないし **show ipv6 interface brief** コマンドの出力で現われないそうではないかもしれません。 **提示 IPv6 VRF がすべての interface コマンド**どのインターフェイスでもこのように設定されたかどうか判別するのに使用することができます。 以下は **提示 IPv6 VRF** の出力バンドルの一部として処理する IPv6 のために設定され、VRF 例に割り当てられるインターフェイスを示す **すべての interface コマンド**です:

```
RP/0/RSP0/CPU0:ASR9006-B#show diag | include PID:
Tue Jan 26 00:07:09.406 EST
  PID:   A9K-RSP440-SE
  PID:   A9K-RSP440-SE
  PID:   A9K-8X100GE-SE
  PID:   A9K-8T-L
  PID:   A9K-36X10GE-SE
  PID:   A9K-MOD160-TR
  PID:   A9K-MPA-8X10GE
  PID:   A9K-MPA-8X10GE
RP/0/RSP0/CPU0:ASR9006-B#
```

脆弱性を含んでいないことが確認された製品

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。

Cisco 集約は Trident ベースのラインカードを含まれないし、Cisco IOS XR ソフトウェア リリース 5.3.4 を実行しなかったり、IPv6 のためにイネーブルになっていない影響を受けていないルータ（ASR）9000 シリーズを保守します。

Cisco IOS XR ソフトウェアを実行するその他のデバイスは影響を受けていません。

セキュリティ侵害の痕跡

この脆弱性の不正利用により Trident ベースの次と同じようなラインカードおよび Generate エラーメッセージはリロードします可能性があります:

```
RP/0/RSP0/CPU0:ASR9006-B#show diag | include PID:
Tue Jan 26 00:07:09.406 EST
  PID:    A9K-RSP440-SE
  PID:    A9K-RSP440-SE
  PID:    A9K-8X100GE-SE
  PID:    A9K-8T-L
  PID:    A9K-36X10GE-SE
  PID:    A9K-MOD160-TR
  PID:    A9K-MPA-8X10GE
  PID:    A9K-MPA-8X10GE
RP/0/RSP0/CPU0:ASR9006-B#
```

最終的な確認に関してはこれらのメッセージが全くこの問題の不正利用を示すかどうか、サポート 組織に連絡して下さい。

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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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。

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

この脆弱性に対処するソフトウェアメンテナンス アップグレード（SMU）は使用できるようにされました。 修正はまた Cisco IOS XR ソフトウェア リリース 5.3.4 のためのサービスパック 7 に組み込まれました。

IOS XR リリース	SMU ID	SMU/Service パック名前
5.3.4	AA13804	asr9k-px-5.3.4.CSCvg46800.tar
5.3.4	AA13870	asr9k-px.5.3.4.sp7.tar

SMU/service パックは Cisco.com の Software Center から **IOS XR ソフトウェア メンテナンスアップデート**へのによってナビゲート ダウンロードすることができます（それぞれ **SMU)-5.3.4** または **IOS XR サービス Packs-5.3.4**。

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-20180131-ipv6

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-January-31

利用規約

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。