Cisco IOS XR Software IPv6 Malformed Packet Denial of Service Vulnerability

Advisory ID: cisco-sa-20140611-ipv6

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140611-ipv6

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。

Revision 1.0

For Public Release 2014 June 11 16:00 UTC (GMT)

目次

要約

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 ソフトウェアには、不正なインターネットプロトコル バージョン 6 (IPv6) パケットを解析する際に脆弱性があります。これにより、認証されていないリモートの攻撃者が、トラフィックを処理するネットワークプロセッサ (NP) チップをロックアップできる可能性があり、その結果としてNP や ラインカードのリロードが発生する場合があります。この脆弱性の影響を受けるのは、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により、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 チップをロックアップさせる可能性があり、その結果としてNP や ラインカードリロード、および 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無償のソフトウェア アップデートをリリースしました。
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、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140611-ipv6

該当製品

脆弱性が認められる製品

Trident ベースのラインカードがインストールされた Cisco ASR 9000 シリーズのルータは、この脆弱性の影響を受けます。IPv6 の設定をしていないデバイスにおいても、この脆弱性の影響を受けます。

Cisco ASR 9000 シリーズの最初の世代のイーサネット ラインカードは、Trident ベースのラインカードと呼ばれています。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 ベースであるかどうかを確認するには、**show diag** コマンドを使用します。該当デバイスには、少なくともいずれかの Trident ベースのカードの PID が含まれています。次の例は、A9K-40GE-B カードがアクティブであるデバイスを示しています。

```
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
```

脆弱性が認められない製品

Typhoon ベースのラインカードのみがインストールされた Cisco ASR 9000 シリーズのルータは、この脆弱性の影響を受けません。
Cisco ASR 9000 シリーズの第 2 世代のイーサネットライン カードは、Typhoon ベースのライン カードと呼ばれています。

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、この脆弱性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 ソフトウェアには、不正なインターネットプロトコル バージョン 6（IPv6）パケットを解析する際に脆弱性があります。これにより、認証されていないリモートの攻撃者が、トラフィックを処理するネットワークプロセッサ（NP）チップをロックアップできる可能性があり、その結果としてNP や ラインカードのリロードが発生する場合があります。この脆弱性の影響を受けるのは、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により、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 チップをロックアップさせる可能性があり、その結果としてNP や ラインカードのリロード、および DoS 状態が発生する可能性があります。

またこの脆弱性が繰り返し不正利用されることにより、長時間にわたって DoS 状態が続きます。

IPv6 の設定をしていないデバイスにおいても、この脆弱性の影響を受けます。Trident ベースのラインカード上に設定されたインターフェースが IPv6 の機能を有効にしていない場合、攻撃者は隣接するホストからのみ不正なトラフィックを送信することが可能です。該当デバイスで IPv6 の機能を有効にしている場合、リモートネットワークからこの脆弱性を不正利用される可能性があります。

ある中間デバイスが不正な IPv6 パケットをブロックしたとしても、不正なパケットがリモートネットワークから送信され、該当デバイスでこの脆弱性が不正利用される可能性はあります。

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）ID として CVE-2014-2176 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCun71928 - Cisco IOS XR Software IPv6 Malformed Packet Denial of Service Vulnerability Calculate the environmental score of

CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、NP チップがロックアップされ、その結果としてNP やラインカードのリロードが発生する可能性があります。

そのカードを通過するすべてのトラフィックが、この状態の影響を受けます。

ソフトウェア バージョンおよび修正

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 Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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 ソフトウェアの SMU で修正されています。

- **asr9k-p-4.2.1.CSCun71928** および **asr9k-px-4.2.1.CSCun71928**（バージョン 4.2.1 用）
- **asr9k-px-4.2.3.CSCun71928** および **asr9k-p-4.2.3.CSCun71928**（バージョン 4.2.3 用）
- **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： その他のバージョンに対応した Cisco IOS XR ソフトウェアの SMU は、利用可能になり次第公開される予定です。

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その他の回避策については、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』で紹介しています。このドキュメントは、次のリンクから入手可能です：http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=33986

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）

- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、E メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（ http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html ）を参照してください。

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不正利用事例とその公表は確認しておりません。

この脆弱性は、カスタマー ケースの調査時に、Cisco TAC によって発見されたものです。

この通知のステータス：FINAL

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証を示唆するものでもありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140611-ipv6

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信さ

れるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-June-11	Initial Public Release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。