# Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ MPLS OAM 用の Cisco IOS XR ソフトウェアで確認されたサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20190515-iosxr-mpls-dos
初公開日 : 2019-05-15 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 : CSCvk63685

CVE-2019-1846

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 ルータ用の Cisco IOS XR ソフトウェアに実装されたマルチプロトコル ラベル スイッチング（MPLS）では、運用、管理、保守（OAM）パケットで脆弱性が確認されました。認証されていない攻撃者が、標的デバイスと隣接したネットワークからサービス妨害（DoS）を仕掛ける危険性があります。

この脆弱性は、特定の MPLS OAM パケットが適切に処理されないことに起因します。悪意のある MPLS OAM パケットを標的デバイスに送信することでエクスプロイトされる可能性があります。エクスプロイトに成功すると、lspv_server プロセスがクラッシュする恐れがあります。クラッシュが発生するとシステムが不安定になるため、デバイスからのトラフィック処理および転送が不可能となり、DoS 状態に陥る危険性があります。通常の運用状態を復元するためには、手動による介入が必要です。

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-20190515-iosxr-mpls-dos

## 該当製品

## 脆弱性のある製品

本脆弱性は、シスコ アグリゲーション サービス ルータ（ASR）9000 シリーズにおいて、次の条件が満たされた場合に影響を及ぼします。

- このルータは Cisco IOS XR ソフトウェア リリース 5.3.3 サービス パック 10 を実行しています。
- ルータには、MPLS OAM 機能が設定されています。

脆弱性が存在する Cisco IOS XR ソフトウェア リリースの詳細については、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。

MPLS OAM が設定されているかどうかの確認

管理者は show running-config mpls oam コマンドを使用して、MPLS OAM が有効になっているかどうかを確認できます。デバイスの MPLS OAM 機能が有効になっている場合、コマンドの出力は以下の例のようになります。

```
<#root>

RP/0/RSP0/CPU0:ASR9001#

show running-config mpls oam


Tue Feb 19 12:45:37.011 UTC

mpls oam
```

このコマンドによる出力がないの場合、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けません。

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。

以下は、Cisco IOS XR ソフトウェア リリース 5.3.3 サービス パック 10 を実行中のデバイスで show version コマンドを実行した場合の出力例です。

```
<#root>

RP/0/RSP0/CPU0:ASR9001#

show version

Wed Jan 24 01:32:32.751 EST


Cisco IOS XR Software, Version 5.3.3

[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-

5.3.3.sp10

-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
```

### 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。

Cisco アグリゲーション サービス ルータ（ASR）9000 シリーズで Cisco IOS XR ソフトウェア リリース 5.3.3 サービス パック 10 を実行していない場合、あるいは MPLS OAM 機能が有効になっていない場合については、この脆弱性の影響を受けないことを確認済みです。注:Cisco XRソフトウェアでは、MPLS OAM機能はデフォルトで有効になっていません。

他のデバイスで、Cisco IOS XR ソフトウェアを実行している場合は影響を受けません。また、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco NX-OS ソフトウェアを実行するデバイスに影響を与えないことも確認しました。

## 詳細

MPLS OAM 機能を使用することで、サービス プロバイダーはラベルスイッチド パス ( LSP ) を監視し、MPLS 転送の問題を迅速に局所化できるため、MPLS ネットワークの障害検出とトラブルシューティングに役立ちます。 この脆弱性は、特定の MPLS OAM パケットが適切に処理されないことに起因します。悪意のある MPLS OAM パケットを標的デバイスに送信することでエクスプロイトされる可能性があります。 脆弱性をエクスプロイトするには、ターゲット デバイスと同じ MPLS ドメインにアクセスし、MPLS OAM パケット処理を設定する必要があります。脆弱性がエクスプロイトされると、lspv_server プロセスがクラッシュする恐れがあります。これにより、DoS 状態に陥り、復元には手動による介入が必要になります。

## セキュリティ侵害の痕跡

脆弱性がエクスプロイトされた場合、対象となるデバイスで、次のようなエラー メッセージが生成される場合があります。

```
#RP/0/RSP0/CPU0:May  14 01:44:57.911 : dumper[60]: %OS-DUMPER-7 DUMP_REQUEST : Dump request for process
 RP/0/RSP0/CPU0:May  14 01:44:57.913 : dumper[60]: %OS-DUMPER-7-DUMP_ATTRIBUTE : Dump request with attr
 RP/0/RSP0/CPU0:May  14 01:44:57.913 : dumper[60]: %OS-DUMPER-4-CRASH_INFO : Crashed pid = 561506 (pkg/
```

脆弱性のエクスプロイトによってデバイスが影響を受けているかどうかを判断するには、サポート担当部門に連絡し、エラーメッセージの調査をご依頼ください。

## 回避策

この脆弱性に対処する回避策はありません。

MPLS OAM 機能を無効にすると、エクスプロイト ベクトルが削除されます。管理者は、グローバル コンフィギュレーション モードで no mpls oam コマンドを使用して、MPLS OAM 機能を無効にすることができます。脆弱性を修正したアップグレードが提供されるまでは、この処置が最善策になります。

## 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。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。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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

シスコでは、この脆弱性に対処する Cisco アグリゲーション サービス ルータ（ASR）9000 シリーズ向けのソフトウェア メンテナンス アップグレード（SMU）もリリースしています。また、Cisco IOS XR ソフトウェア リリース 5.3.3 のサービス パック 11 にも修正が含まれています。

| IOS XR リリース | SMU ID | ASR 9000 SMU 名 |
|---|---|---|
| 5.3.3 | AA14582 | asr9k-px-5.3.3.CSCvk63685 |

SMU やサービス パックは、Cisco.com の Software Center からダウンロードできます。

## 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。

## 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-20190515-iosxr-mpls-dos

## 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 | 2019 年 5 月 15 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。