

Cisco ASR 903 アグリゲーション サービス ルータ用 Cisco IOS XE ソフトウェアの ARP における サービス妨害 (DoS) の脆弱性



アドバイザリーID : cisco-sa-asr903-rsp3-[CVE-2025-arp-dos-WmfzdvJZ](#)
[20189](#)

初公開日 : 2025-05-07 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 : [CSCwh55442](#)

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

ルートスイッチプロセッサ 3 (RSP3C) を搭載した Cisco ASR 903 アグリゲーション サービス ルータ用の Cisco IOS XE ソフトウェアの Cisco Express Forwarding (CEF) 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。

この脆弱性は、Cisco IOS XE ソフトウェアが Address Resolution Protocol (ARP) メッセージを処理する際の不適切なメモリ管理に起因します。攻撃者は、巧妙に細工された ARP メッセージを一定期間にわたって該当デバイスに高頻度で送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はシステムリソースを使い果たし、最終的にアクティブなルートスイッチプロセッサ (RSP) のリロードを引き起こす可能性があります。冗長 RSP がない場合、ルータがリロードされます。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr903-rsp3-arp-dos-WmfzdvJZ>

このアドバイザリーは、2025 年 5 月に公開された Cisco IOS ソフトウェアおよび IOS XE ソフトウェアリリースのセキュリティ アドバイザリー バンドルの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: May 2025 Semiannual Cisco IOS and IOS XE 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、デバイス設定に関係なく、Cisco IOS XE ソフトウェアの脆弱性のあるリリースを実行する、RSP3C 搭載の Cisco ASR 903 アグリゲーション サービス ルータに影響を与えます。

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。

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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 (RSP3C 搭載の Cisco ASR 903 アグリゲーション サービス ルータ以外のデバイスで実行されている場合)
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

セキュリティ侵害の痕跡

uea_mgr プロセスの RSS メモリ使用量をモニターするには、show process memory platform sorted | include RSS|uea_mgr コマンドの出力を表示します。通常の状態では、以下の例に示すように、uea_mgr プロセスの RSS メモリ使用量は約 1 GB (1,048,576 バイト) です。

<#root>

Router#

show process memory platform sorted | include RSS|uea_mgr

Pid	Text	Data	Stack	Dynamic
-----	------	------	-------	---------

RSS

		Name				
2366	1525	948416	136	71960	948416	uea_mgr

Router#

uea_mgr プロセスの RSS メモリ使用量が 1,048,576 バイトを超える場合は、この脆弱性がエクスプロイトされている可能性があります。uea_mgr プロセスの RSS メモリ使用量が約 1.7 GB (1,782,580 バイト) に達すると、予期しない RSP のリロードが発生することが確認されています。

回避策

この脆弱性に対処する回避策はありません。

ただし、この脆弱性のエクスプロイトが成功した結果として発生する予期せぬリロードを回避するため、このアドバイザリの「[セキュリティ侵害の痕跡](#)」セクションに記載されているように、uea_mgr プロセスの RSS メモリ使用量をモニターできます。その後、メモリ使用量がクリティカルレベルに達する前に、RSP のリロードを計画的にスケジュールできます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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です。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 (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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS および IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは [Cisco Software Checker](#) を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース (「First Fixed」) を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース (「Combined First Fixed」) を特定できます。

このツールを使用するには、「[Cisco Software Checker](#)」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、[セキュリティ影響評価 \(SIR \)](#) が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号 (例 : 15.9(3)M2、17.3.3) を入力します。
3. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		
Enter release number	Check	

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-asr903-rsp3-arp-dos-WmfzdvdvJZ>

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	2025 年 5 月 7 日

利用規約

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も示唆するものではありません。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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

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、単独の転載や意識を施した場合、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。

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。