ASR 1000 シリーズ 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 IPv6 マルチキャスト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-mlre-H93FswRz
初公開日 : 2023-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwe91722

CVE-2023-20187

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 1000 シリーズ アグリゲーション サービス ルータ用の Cisco IOS XE ソフトウェアのマルチキャスト リーフ リサイクル排除（mLRE）機能における脆弱性により、認証されていないリモート攻撃者が該当デバイスのリロードを引き起こし、結果としてサービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、該当デバイスで特定の IPv6 マルチキャストパケットが 8 回以上ファンアウトされた場合にそれらのパケットが不適切に処理されることに起因します。攻撃者は、該当デバイスを介して特定の IPv6 マルチキャストまたは IPv6 マルチキャスト VPN（MVPNv6）パケットを送信することにより、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、攻撃者が該当デバイスのリロードを引き起こし、結果としてサービス妨害（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ソフトウェアアップデートをリリースしています。本脆弱性に対処する回避策がいくつかあります。

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-mlre-H93FswRz

このアドバイザリは、2023 年 9 月に公開された Cisco IOS および IOS XE ソフトウェア セキュリティ アドバイザリ バンドルの一部です。アドバイザリとリンクの一覧については、『

Cisco Event Response: September 2023 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、次の条件がすべて満たされた場合に、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに影響を与えます。

- Cisco IOS XE ソフトウェアの該当リリースをデバイスが実行している。
- 次のいずれかの Embedded Services Processor（ESP）または統合 ESP がデバイスに搭載されている。
  - ASR1000-ESP40
  - ASR1000-ESP100
  - ASR1000-ESP200
  - ASR1001-X
  - ASR1001-HX
  - ASR1002-X
  - ASR1002-HX
- デバイスで IPv6 マルチキャストまたは IPv6 マルチキャスト VPN が設定されており、ipv6 multicast-routing が設定されている。
- IPv6 マルチキャストパケットが 8 回以上ファンアウトされるようにデバイスが設定されている：デバイスで設定されている IPv6 マルチキャストパケットのファンアウト回数を確認するには、CLI コマンド show ipv6 mfib IPv6 group address を使用します。次の例は、IPv6 マルチキャストパケットを 8 回ファンアウトするように設定されているため影響を受けるデバイスの CLI 出力を示しています。
  <#root>

```
Router#

show ipv6 mfib IPv6 group address


(2001:DB8:FFFF:48::5:FFFF,FF3E::9800:200) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   5/0/110/0, Other: 0/0/0
   GigabitEthernet2/1/1 Flags: A
   Port-channel1.8 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.7 Flags:

F

 IC NS
```

```
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.6 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.5 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.4 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.3 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.2 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps
   Port-channel1.1 Flags:

F

 IC NS
     Pkts: 0/0/0    Rate: 0 pps

8 F interfaces
```

- デバイスで Cisco mLRE が有効になっている。
  注：mLRE は、すべての該当プラットフォームにおいてデフォルトで有効になっています。mLRE が無効になっている場合、show running-config コマンドの出力には platform multicast lre off が含まれます。次の例のように、Cisco IOS XE ソフトウェアリリース 17.1.1 以降では、管理者は、show platform hardware qfp active feature multicast lre コマンドを使用して mLRE のステータスを確認できます。
  <#root>

```
Router#

show platform hardware qfp active feature multicast lre


=== mcast lre config ===
  Platform v4mcast LRE config: On
  Platform v6mcast LRE config: On
Router#
```

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。

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 XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

また、シスコでは、次の ESP モデルが動作しているすべての Cisco ASR 1000 シリーズ アグリゲーション サービス ルータがこの脆弱性の影響を受けないことを確認しています。

- ASR1000-ESP100-X
- ASR1000-ESP200-X

回避策

次の例のように、管理者は、該当デバイスで mLRE を無効にすることができます。

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#platform multicast lre off
Router(config)#end
Router#show platform hardware qfp active feature multicast lre
=== mcast lre config ===
Platform v4mcast LRE config: Off
Platform v6mcast LRE config: Off
Router#
```

mLRE 機能が無効になっている場合、パケットは、マルチキャストトラフィックを複製する異なるインターフェイスに対して個別に処理されます。mLRE と mLRE を無効にした場合の影響の詳細については、『mLRE Feature on the IOS-XE Router』を参照してください。

この回避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。

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アップグレード ソリューション一式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 ソフトウェアおよび 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（15.9(3)M2、17.3.3 など）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-mlre-H93FswRz

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	2023 年 9 月 27 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。

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。