Intermediate System-to-Intermediate SystemのCisco IOS XRソフトウェアセグメントルーティング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-isis-xehpbVNe CVE-2024-20406
初公開日 : 2024-09-11 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 : CSCwi39542

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 IOS XRソフトウェアのIntermediate System-to-Intermediate System(IS-IS)プロトコルのセグメントルーティング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該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、入力IS-ISパケットの不十分な入力検証に起因します。攻撃者は、アジャセンシー関係を形成した後、該当デバイスに特定のIS-ISパケットを送信することで、この脆弱性を不正利用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、Flexible Algorithm（FA；柔軟アルゴリズム）に参加しているすべての該当デバイスでIS-ISプロセスをクラッシュさせて再起動させ、DoS状態を引き起こす可能性があります。

注：IS-IS プロトコルはルーティングプロトコルです。この脆弱性を不正利用するには、攻撃者は該当デバイスとレイヤ2で隣接関係を形成している必要があります。この脆弱性は、IPv4およびIPv6コントロールプレーン上のIS-ISのセグメントルーティング、およびレベル1、レベル2、またはマルチレベルルーティングIS-ISタイプとして設定されているデバイスに影響を与えます。

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-isis-xehpbVNe

このアドバイザリは、2024年9月に公開されたCisco IOS XR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 2024 Semiannual Cisco IOS XR 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、Cisco IOS XRソフトウェアの脆弱性が存在するリリースを実行していて、IS-ISセグメントルーティングの柔軟なアルゴリズム(SRA)が有効にされていて、次の機能も有効になっているシスコプラットフォームに影響を与えます。

- セグメントルーティングマイクロループの回避
- 柔軟なアルゴリズムのためのTopology Independent Loop-Free Alternate(TI-LFA)

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。

デバイスの設定に脆弱性があるかどうかの確認

デバイスに脆弱性のある設定があるかどうかを確認するには、次の手順に従います。デバイスでIS-IS Segment Routing Flexible Algorithm(SRALG)が有効であっても、マイクロループ回避やTI-LFAが有効になっていない場合、この脆弱性の影響を受けません。

1. IS-ISセグメントルーティングフレキシブルアルゴリズムのステータスを確認する

デバイスでIS-IS Segment Routing Flexible Algorithm(SRR)が有効になっているかどうかを確認するには、show running-config router isis | | include flex-algo EXECコマンドを使用します。デバイスがIS-IS Segment Routing Flexible Algorithm用に設定されている場合、このコマンドは出力を返します。次の例は、IS-IS Segment Routing Flexible Algorithm(SLR)用に設定されたデバイスの出力の一部を示しています。

<#root>

```
RP/0/RSP0/CPU0:XR#
show running-config router isis | include flex-algo

Wed Sept 11 16:00:00.000 UTC
flex-algo 200
RP/0/RSP0/CPU0:XR#
```

デバイスが出力を返す場合、この脆弱性の影響を受ける可能性があります。ステップ 2 に進みます。

デバイスから出力が返されない場合、この脆弱性の影響を受けません。手順2または手順3を完了する必要はありません。

2. IS-ISセグメントルーティングマイクロループ回避ステータスの判別

デバイスでIS-IS Segment Routing Microloop Avoidance(SRE)が有効になっているかどうかを確認するには、show running-config router isis | | include microloop EXECコマンドを使用します。デバイスがIS-IS Segment Routing Microloop Avoidanceに設定されている場合、このコマンドは出力を返します。次の例は、IS-ISセグメントルーティングマイクロループ回避が設定されたデバイスでの出力の一部を示しています。

```
<#root>

RP/0/RSP0/CPU0:XR#

show running-config router isis | include microloop


Wed Sept 11 16:00:00.000 UTC
  microloop avoidance segment-routing
RP/0/RSP0/CPU0:XR#
```

デバイスが出力を返し、IS-IS Segment Routing Flexible Algorithm(SRALGORITHM)が有効になっている場合、この脆弱性の影響を受けます。

デバイスから出力が返されない場合は、IS-ISセグメントルーティングマイクロループ回避(SRE)が有効になっていません。ステップ 3 に進みます。

3. Flexible AlgorithmステータスのTI-LFAの判別

デバイスでFlexible Algorithm(FLEXIBLE)用のTI-LFAが有効になっているかどうかを確認するには、show running-config router isis | include ti-lfa EXECコマンドを使用することで確認できます。デバイスがIS-IS TI-LFA用に設定されている場合、このコマンドは出力を返します。次の例は、Flexible AlgorithmのIS-IS TI-LFA用に設定されたデバイスでの出力の一部を示しています。

```
<#root>

RP/0/RSP0/CPU0:XR#

show running-config router isis | include ti-lfa


Wed Sept 11 16:00:00.000 UTC
   fast-reroute per-prefix ti-lfa
RP/0/RSP0/CPU0:XR#
```

デバイスが出力を返し、IS-IS Segment Routing Flexible Algorithm(SRALGORITHM)が有効になっている場合、この脆弱性の影響を受けます。

デバイスから出力が返されない場合は、Flexible Algorithm(FM)のIS-IS TI-LFAが有効になっていないため、この脆弱性の影響を受けません。

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 XE ソフトウェア
- NX-OS ソフトウェア

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、緩和策があります。

ベストプラクティスとして、IS-IS エリア認証を設定して、攻撃者がこの脆弱性をトリガーするために認証に合格する必要があるようにします。IS-IS 認証の詳細については、「IS-IS 認証の設定」を参照してください。

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。

修正済みリリース

次の表では、左の列にシスコソフトウェアリリースまたはトレインを示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
6.7.4 以前	影響なし。
6.8	修正済みリリースに移行。
6.9	修正済みリリースに移行。
7.0 ~ 7.3	影響なし。
7.4 ~ 7.10	修正済みリリースに移行。
7.11	7.11.2

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
24.1 以降	影響なし。

シスコはこの脆弱性に対処する次の SMU もリリースしています。一覧に記載されていないプラットフォームやリリース向けの SMU を必要とするお客様は、サポート部門にご連絡ください。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.5.2	8000 シリーズ ASR9K-X64 NCS540 NCS540L NCS5500 NCS560	8000-7.5.2.CSCwi39542 asr9k-x64-7.5.2.CSCwi39542 ncs540-7.5.2.CSCwi39542 ncs540l-7.5.2.CSCwi39542 ncs5500-7.5.2.CSCwi39542 ncs560-7.5.2.CSCwi39542
7.7.2	8000 シリーズ ASR9K-X64	8000-7.7.2.CSCwi39542 asr9k-x64-7.7.2.CSCwi39542
7.9.2	8000 シリーズ ASR9K-X64 NCS5500	8000-7.9.2.CSCwi39542 asr9k-x64-7.9.2.CSCwi39542 ncs5500-7.9.2.CSCwi39542
7.9.21	ASR9K-X64	asr9k-x64-7.9.21.CSCwi39542
7.10.2	8000 シリーズ ASR9K-X64	8000-7.10.2.CSCwi39542 asr9k-x64-7.10.2.CSCwi39542

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

出典

この脆弱性は、シスコの内部セキュリティテストでPrathap Raju Hongere Debaraju氏によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-xehpbVNe

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	2024年9月11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。