Cisco IOS XRソフトウェアのMulti-Instance Intermediate System-to-Intermediate Systemにおける DoS脆弱性

アドバイザリーID : cisco-sa-isis-dos-kDMxpSzK
初公開日 : 2026-03-11 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 : CSCwq71827

CVE-2026-20074

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)マルチインスタンスルーティング機能の脆弱性により、認証されていない隣接する攻撃者がIS-ISプロセスを予期せず再起動させる可能性があります。

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、巧妙に細工されたIS-ISパケットを該当デバイスに送信することで、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IS-ISプロセスを予期せず再起動させ、アドバタイズされたネットワークへの接続を一時的に失い、サービス拒否(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。この脆弱性をエクスプロイトするには、攻撃者は影響を受けるデバイスとレイヤ 2 隣接関係にあり、隣接関係を形成済みである必要があります。

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。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-dos-kDMxpSzK

このアドバイザリは、Cisco IOS XRソフトウェアSecurity Advisoryバンドル公開の2026年3月リリースの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: March

2026 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マルチインスタンスルーティング機能が有効になっているシスコデバイスに影響を与えます。

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。

デバイスの設定に脆弱性があるかどうかの確認

デバイスでIS-ISマルチインスタンスルーティングが設定されているかどうかを確認するには、show running-config router isis | include instance-id EXECコマンドを使用します。コマンドが少なくとも1つのインスタンスIDを返す場合、デバイスはIS-ISマルチインスタンスルーティング用に設定されており、次の例に示すとおり、この脆弱性の影響を受けます。

<#root>

```
RP/0/RP0/CPU0:ios#
show running-config router isis | include instance-id

Mon Feb  9 17:30:18.448 UTC
 instance-id 1
RP/0/RP0/CPU0:ios#
```

コマンドで出力が返されない場合、デバイスは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
- 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。

緩和策として、IS-ISエリア認証を設定します。この脆弱性を悪用するには、隣接関係を形成する前に、攻撃者がIS-ISエリアへの認証に成功する必要があります。IS-IS認証の設定の詳細については、『Cisco NCS 5500シリーズルータ、IOS XRリリース24.1.x、24.2.x、24.3.x、24.4.xのルーティングコンフィギュレーションガイド』の「IS-IS認証」セクション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。お客様固有の導入シナリオおよび制限によっては、緩和策を導入すると、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。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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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記載しています。右側の列は、リリース（トレイン）がこのアドバイザリに記載されている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）
7.7 以前	影響なし。
7.8	修正済みリリースに移行。
7.9	修正済みリリースに移行。
7.10	修正済みリリースに移行。
7.11	修正済みリリースに移行。
24.1	修正済みリリースに移行。
24.2	修正済みリリースに移行。
24.3	修正済みリリースに移行。
24.4	修正済みリリースに移行。
25.1	修正済みリリースに移行。

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）
25.2	25.2.2
25.3	25.3.1
25.4	影響なし。

SMU もこの脆弱性に対処するために使用できます。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。この脆弱性に関して公開されている可能性がある SMU の特定方法の詳細については、『Cisco IOS XR ソフトウェア メンテナンス アップデート（SMU）について』の「ダウンロード」セクションを参照してください。

シスコの 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済み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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

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

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	2026年3月11日

利用規約

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。