Cisco IOS XR ソフトウェアのインターネット キー エクスチェンジ バージョン 2 におけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-xrike-9wYGpRGq
初公開日 : 2025-03-12 16:00
バージョン 1.0 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwk64612

CVE-2025-20209

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 ソフトウェアのインターネット キー エクスチェンジ バージョン 2（IKEv2）機能で脆弱性が確認されました。認証されていないリモートからの攻撃者によって、該当デバイスでコントロールプレーンの UDP パケットを処理できなくなる危険性があります。

この脆弱性は、不正な形式の IKEv2 パケットの不適切な処理に起因します。攻撃者は、該当デバイスに不正な形式の IKEv2 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、攻撃者は該当デバイスでコントロールプレーンの UDP パケットを処理できないようにし、その結果、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。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-xrike-9wYGpRGq

このアドバイザリは、2025 年 3 月に公開された Cisco IOS XR ソフトウェアリリースのセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、Cisco Event Response: March 2025 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おり、IKEv2 が有効になっている以下のシスコ製品に影響を与えます。

- Network Convergence System（NCS）540L
- NCS 1004
- NCS 1010
- NCS 1014

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。

デバイス設定の確認

デバイスで IKEv2 が設定されているかどうかを判断するには、show udp brief コマンドを使用して、デバイスがポート 4500 および 500 でリッスンしているかどうかを確認します。次に、この脆弱性に該当するデバイス上での CLI 出力の表示例を示します。

<#root>

```
Router#
show udp brief


   PCB           VRF-ID     Recv-Q Send-Q Local Address      Foreign Address
0x000000000000 0x60000000      0      0  0.0.0.0:4500       0.0.0.0:0
0x000000000000 0x00000000      0      0  0.0.0.0:4500       0.0.0.0:0
0x000000000000 0x60000000      0      0  0.0.0.0:500        0.0.0.0:0
0x000000000000 0x00000000      0      0  0.0.0.0:500        0.0.0.0:0
Router#
```

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
- 脆弱性が存在するものとして記載されていないその他の IOS XR ソフトウェア製品

回避策

この脆弱性に対処する回避策はありません。

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。

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）
7.10 以前	修正済みリリースに移行。
7.11	7.11.21
24.1	修正済みリリースに移行。
24.2	24.2.2
24.3 以降	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。

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 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-xrike-9wYGpRGq

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 3 月 12 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。