Cisco IOS XRソフトウェアのBorder Gateway Protocolコンフェデレーションにおける Denial of Service(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-iosxr-bgp-dos-O7stePhX
CVE-2025-20115
初公開日 : 2025-03-12 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwk15887

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ソフトウェアのボーダーゲートウェイプロトコル(BGP)におけるコンフェデレーション（連携）実装の脆弱性により、認証されていないリモートの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、255個の自律システム番号（AS番号）を持つAS_CONFED_SEQUENCE属性を使用してBGPアップデートを作成する際に発生するメモリ破損に起因します。 攻撃者は、巧妙に細工されたBGPアップデートメッセージを送信することによってこの脆弱性を不正利用する可能性があります。または、AS_CONFED_SEQUENCE属性が255以上のAS番号に増加するようにネットワークが設計されている可能性があります。エクスプロイトに成功すると、攻撃者はメモリを破損させ、BGPプロセスの再起動を引き起こし、その結果DoS状態が発生する可能性があります。この脆弱性を不正利用するには、攻撃者が標的と同じ自律システム内のBGPコンフェデレーションスピーカを制御する必要があります。または、AS_CONFED_SEQUENCE属性が255以上のAS番号に拡大するようにネットワークが設計されている必要があります。

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-iosxr-bgp-dos-O7stePhX

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2025年3月リ

リースの一部です。これらのアドバイザリとリンクの一覧については、シスコイベントレスポンス：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公開の半年刊2025年3月を参照してください。

該当製品

脆弱性のある製品

公開時点で、Cisco IOS XRソフトウェアにBGPコンフェデレーションが設定されている場合、この脆弱性の影響を受けました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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BGPコンフェデレーションが設定されているかどうかを確認するには、show running-config router bgp EXEC CLIコマンドを使用します。ルータが BGP 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。脆弱性が存在すると見なされるデバイスについては、次の例に示すように、bgp confederation peers設定コマンドが出力に表示されている必要もあります。

<#root>

```
# show running-config router bgp

router bgp 64500
.
.
.
bgp confederation peers
```

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。この脆弱性は、BGP AS_CONFED_SEQUENCEアトリビュートが255以上のAS番号であることにも起因しています。回避策は、このBGPアトリビュートを254以下のAS番号に制限することです。これは、コンフェデレーションピア上で、長いASパス長を持つBGPアップデートをドロップするルーティングポリシーを使用して実現できます。

<#root>

```
route-policy
```

max-asns

```
  if as-path length ge 254 then
      drop
  else
      pass
  endif
end-policy

router bgp 64500
 bgp confederation peers
  64501
  64502
 !
bgp confederation identifier 64511 neighbor 192.168.0.1
 remote-as 64501
  address-family ipv4 unicast
```

policy max-asns in

policy max-asns out

Cisco IOS XRのルーティングポリシー言語(RPL)の詳細については、『Implementing Routing Policy on Cisco IOS XR Software』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

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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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）
7.11 以前	修正済みリリースに移行。
24.1 以前	修正済みリリースに移行。
24.2	24.2.21 (future release)
24.3	24.3.1
24.4	影響なし。

この脆弱性に対処するためにSMUも使用できます。使用できないプラットフォームまたはリリースでSMUを必要とするお客様は、サポート組織に連絡することをお勧めします。この脆弱性に対して公開されている可能性があるSMUを見つける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、この問題に関する公式発表を認識しています。このアナウンスはCisco IOS XRソフトウェアに固有のものではなく、『BGPでの無限AS-PATHSの作成』で確認できます。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

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-iosxr-bgp-dos-O7stePhX

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。