

Cisco IOS XEソフトウェアのNetwork-Based Application Recognition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-nbar-dos-LAvwTmeT

[CVE-2025-20315](#)

初公開日 : 2025-09-24 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwn46756](#)

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 XEソフトウェアのNetwork-Based Application Recognition(NBAR)機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こし、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。

この脆弱性は、不正なControl and Provisioning of Wireless Access Points(CAPWAP)パケットの不適切な処理に起因します。攻撃者は、該当デバイスを介して不正なCAPWAPパケットを送信することにより、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、攻撃者はデバイスの予期しないリロードを引き起こすことが可能になり、結果として 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。ただし、緩和策があります。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nbar-dos-LAvwTmeT>

このアドバイザリーは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリーバンドル公開の2025年9月リリースの一部です。これらのアドバイザリー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およびIOS XEソフトウェアに関するセキュリティアドバイザリー公開資料 \(半年刊、2025年9月 \)](#)』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 XEソフトウェアの脆弱性が存在するリリースを実行し、CAPWAP機能のNBARが有効になっている次のシスコ製品に影響を与えます。

- 1100 サービス統合型ルータ
- 4000 シリーズ サービス統合型ルータ
- ASR 920 シリーズ アグリゲーション サービス ルータ
- ASR 1000 シリーズ アグリゲーション サービス ルータ
- Catalyst 1101高耐久性ルータ
- Catalyst 8000V エッジソフトウェア
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Catalyst 8500 エッジプラットフォーム
- Catalyst 8500L エッジプラットフォーム
- Catalyst IR8300 高耐久性シリーズ ルータ

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

特定のデバイスでNBARのCAPWAP検査が有効になっているかどうかを確認するには、show running-config | include tunneled-traffic capwap CLIコマンドを使用します。このコマンドの出力がある場合は、次の例に示すように、NBARのCAPWAPインスペクションが有効になっています。

```
<#root>
```

```
Router#
```

```
show running-config | include tunneled-traffic capwap
```

```
ip nbar classification tunneled-traffic capwap
```

```
Router#
```

出力されない場合、デバイスはこの脆弱性の影響を受けません。

それ以外の場合は、show ip nbar control-plane | include NBAR state CLIコマンドで状態がACTIVATEDと表示されることを確認して、NBARがデバイスで使用されているかどうかを判断します。このコマンドで出力が生成されない場合、または状態がDEACTIVATEDと報告され

る場合、NBAR操作は設定されていません。

次の例は、NBARが有効になっているデバイスの出力を示しています。

```
Router#show ip nbar control-plane | include NBAR state
NBAR state is ACTIVATED
NBAR state: ACTIVATED
```

次の例は、NBARが無効になっているデバイスの出力を示しています。

```
Router#show ip nbar control-plane | include NBAR state
NBAR state is DEACTIVATED
NBAR state: DEACTIVATED
```

NBARのCAPWAPインスペクションが両方とも有効で、NBARがACTIVATEDの場合、そのデバイスは脆弱であると見なされます。

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 XR 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、緩和策として、NBARのCAPWAPインスペクションを無効にするには、グローバルコンフィギュレーションCLIコマンドno ip nbar classification tunneled-traffic capwapを使用します。

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

シスコでは、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、回避策や緩和策は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復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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（例：15.9(3)M2、17.3.3）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-nbar-dos->

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9月24日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。