

# Cisco IOS XEソフトウェアのIPv4フラグメンテーションリアセンブルにおけるDenial of Service(DoS)の脆弱性



アドバイザーID : cisco-sa-cpp-vfr-dos-nhHKGgO

[CVE-2024-20467](#)

初公開日 : 2024-09-25 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 : [CSCwh44152](#)

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IPv4フラグメンテーション再構成コードの実装における脆弱性により、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、フラグメントの再構成時におけるリソースの不適切な管理に起因します。攻撃者は、該当デバイスに特定サイズのフラグメント化されたパケットを送信するか、該当デバイスのVirtual Fragmentation Reassembly(VFR)対応インターフェイスを介して、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

注 : この脆弱性は、Cisco IOS XEソフトウェアリリース17.12.1または17.12.1aを実行しているCisco ASR 1000シリーズアグリゲーションサービスルータおよびCisco cBR-8コンバインドブロードバンドルータに影響を与えます。

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-cpp-vfr-dos-nhHKGgO>

このアドバイザーは、Cisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザーバンドル公開の2024年9月リリースの一部です。アドバイザーとリンクの一覧については

、『[Cisco Event Response: September 2024 Semiannual Cisco IOS and IOS XE 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 XEソフトウェアリリース17.12.1または17.12.1aを実行しているCisco ASR 1000シリーズアグリゲーションサービスルータおよびCisco cBR-8コンバインドブロードバンドルータに影響を与えます。

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。

### デバイス設定の確認

VFR機能が有効になっているかどうかを確認するには、以下の例に示すように、show ip virtual-reassemblyのCLIコマンドを使用します。

```
<#root>
Router#
show ip virtual-reassembly

GigabitEthernet0/0/1:

Virtual Fragment Reassembly (VFR) is ENABLED [in]

    Concurrent reassemblies (max-reassemblies): 16
    Fragments per reassembly (max-fragments): 32
    Reassembly timeout (timeout): 3 seconds
    Drop fragments: OFF
.
.
.
Tunnel1:

Virtual Fragment Reassembly (VFR) is ENABLED

[in]
    Concurrent reassemblies (max-reassemblies): 16
    Fragments per reassembly (max-fragments): 32
    Reassembly timeout (timeout): 3 seconds
    Drop fragments: OFF
```

前記の例では、物理インターフェイスGigabitEthernet0/0/1とトンネルインターフェイス

Tunnel1の両方でVFR機能が有効になっています。これは、両方のインターフェイスがこの脆弱性の影響を受けることを示します。

注: : VFR は、ネットワークアドレス変換 (NAT)、ゾーンベースのファイアウォール、IPSec などの機能によって、レイヤー 4 またはレイヤー 7 の情報を処理するために自動的に有効にされます。VFR を無効にすることは推奨されません。ip virtual-reassembly コンフィギュレーション コマンドは、VFR 機能を手動で有効にしていない限り、show running-config の出力には表示されません。詳細については、「[IP Addressing: Fragmentation and Reassembly Configuration Guide](#)」を参照してください。

## 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 XR ソフトウェア
- Meraki 製品
- 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。

## 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です。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](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。

### Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび 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 ( 15.9(3)M2、17.3.3 など ) 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-cpp-vfr-dos-nhHKGgO>

## 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25日

## 利用規約

本アドバイザリ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。本アドバイザリ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。

本アドバイザリ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。