

# Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの ICMPv6 メッセージ処理におけるサービス妨害の脆弱性



アドバイザリーID : cisco-sa-asa-icmpv6-t5TzqwNd [CVE-2023-20086](#)

初公開日 : 2023-11-01 16:00

最終更新日 : 2023-11-02 13:50

バージョン 1.1 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwd77581](#)

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 適応型セキュリティアプライアンス ( ASA ) ソフトウェアおよび Cisco Firepower Threat Defense ( FTD ) ソフトウェアの ICMPv6 処理の脆弱性により、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、ICMPv6 メッセージの不適切な処理に起因します。攻撃者は、IPv6 が有効になっているターゲットの Cisco ASA または FTD システムに細工された ICMPv6 メッセージを送信することで、この脆弱性を不正利用する可能性があります。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。

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-asa-icmpv6-t5TzqwNd>

このアドバイザリーは、2023 年 11 月に公開された Cisco ASA、FTD、および FMC のセキュリティアドバイザリーバンドルに含まれています。アドバイザリーとリンクの一覧については、[Cisco Event Response : 2023 年 11 月に公開された Cisco ASA、FMC、および FTD ソフトウェアセキュリティアドバイザリーバンドル \( 半期 \)](#) を参照してください。

# 該当製品

## 脆弱性のある製品

この脆弱性の影響を受けるのは、Cisco ASA ソフトウェアおよび FTD ソフトウェアで IPv6 プロトコルが設定されている場合です。

注：IPv4 インターフェイスのみが設定されているデバイスは影響を受けません。

## デバイス設定の確認

該当するソフトウェアリリースを実行し、IPv6 が有効になっているデバイスで IPv6 アドレスが割り当てられているインターフェイスを特定するには、次の例に示すように、show ipv6 interface brief CLI コマンドを使用します。

```
<#root>
ciscocodevice#
show ipv6 interface brief

GigabitEthernet0/0 [up/up]
  2001:db8:32:16:::1
  fdf8:f53b:82e4::53
management [up/up]
  unassigned
```

IPv6 が有効化されている場合、設定に ipv6 enable インターフェイス コンフィギュレーション コマンドが存在します。脆弱性の影響を受ける設定の出力例を以下に示します。

```
<#root>
ciscocodevice#
show running-config interface

interface GigabitEthernet0/0
  ...
  ipv6 enable
  ...
```

## 脆弱性を含ま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 Cisco Firepower Management Center ( FMC ) ソフトウェアに影響を及ぼさないことを確認しました。

## 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ン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 ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスク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。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。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。すべてのアドバイザリ、[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、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [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	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

FTD デバイスのアップグレード手順については、[Cisco Firepower Management Center アップグレードガイド](#)を参照してください。

## 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

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-asa-icmpv6-t5TzqwNd>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Cisco Software Checker フォームを更新。	修正済みソフトウェア	Final	2023年11月2日
1.0	初回公開リリース	—	Final	2023年11月1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。