

# シスコFirepower2100シリーズファイアウォール向けCiscoFirepower脅威対策ソフトウェアのインスペクションルールにおけるDoS脆弱性



アドバイザーID : cisco-sa-ftd-intrusion-dos-DfT7wyGC [CVE-2023-20244](#)

初公開日 : 2023-11-01 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 : [CSCwe98687](#)

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

シスコFirepower2100シリーズファイアウォール向けCiscoFirepower脅威対策(FTD)ソフトウェアの内部パケット処理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、特定のパケットがインスペクションエンジンに送信される際の不適切な処理に起因します。攻撃者は、細工された一連のパケットを該当デバイスに送信することにより、この脆弱性をエクスプロイトする危険性があります。エクスプロイトに成功すると、攻撃者はデバイス上の9,472バイトブロックをすべて使い果たし、デバイス全体でトラフィックが失われたり、予期しないデバイスのリロードが発生したりする可能性があります。デバイスが自動的にリロードしない場合、この状態から回復するには、デバイスを手動でリロードする必要があります。

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-ftd-intrusion-dos-DfT7wyGC>

このアドバイザーは、Cisco ASA、FTD、およびFMCセキュリティアドバイザーバンドル公開の2023年11月版リリースの一部です。アドバイザーの完全なリストとそのリンクについては、『[Cisco Event Response: November 2023 Semiannual Cisco ASA, FMC, and FTD 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 FTDソフトウェアの脆弱性が存在するリリースを実行し、次のいずれかの機能が有効になっているCiscoFirepower2100シリーズファイアウォールに影響を与えます。

- 侵入ポリシー
- マルウェアおよびファイルポリシー
- セキュリティインテリジェンス
- URL フィルタリング

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

影響を受ける機能のいずれかがデバイスで有効になっているかどうかを確認するには、次のいずれかの設定ガイドの該当する章を参照してください。

CiscoFirepowerマネジメントセンター(FMC)によって管理されるCisco FTDデバイス用

- 侵入ポリシー： [侵入ポリシーの概要](#)
- マルウェアおよびファイルポリシー： [ネットワークマルウェア防御およびファイルポリシー](#)
- セキュリティインテリジェンス： [セキュリティインテリジェンス](#)
- URLフィルタリング： [URLフィルタリング](#)

CiscoFirepowerデバイスマネージャ(FDM)を使用したスタンドアロンCisco FTDデバイスの場合

- 侵入ポリシー： [侵入ポリシー](#)
- マルウェアおよびファイルポリシー： [アクセス制御>侵入、ファイル、およびマルウェアの検査](#)
- セキュリティインテリジェンス： [セキュリティインテリジェンス](#)
- URLフィルタリング： [アクセスコントロール> URLフィルタリング](#)

## 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。

- 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア
- Firepower Management Center ( FMC ) ソフトウェア
- 次世代侵入防御システム ( NGIPS )

## セキュリティ侵害の痕跡

CLIコマンドshow blocksの出力に含まれる9,472バイトブロックの空きカウント(CNT)がゼロの場合は、次の例に示すように、この脆弱性が不正利用されている可能性があります。

```
<#root>
```

```
>
```

```
show blocks
```

SIZE	MAX	LOW	
CNT			
0	2700	2700	2700
4	100	100	100
80	1747	1746	1747
256	4148	4142	4143
1550	6234	6231	6232
2048	100	100	100
2560	164	164	164
4096	100	100	100
8192	100	100	100
9472			
24000	0		
0			
16384	100	100	100
65536	16	11	16

Cisco FTDソフトウェアリリース7.0.1以降では、次の例に示すように、show blocks CLIコマンドの出力に9,472バイトブロックのゼロ以外のFAILEDカウントが存在し、さらにフリーカウント(CNT)がゼロの場合に、この脆弱性が悪用されたことを示しています。

```
<#root>
```

```
>
```

```
show blocks
```

SIZE	MAX	LOW	
CNT	FAILED		

0	2700	2699	2700	0
4	100	100	100	0
80	1000	998	1000	0
256	5784	5647	5679	0
1550	6234	6214	6232	0
2048	100	100	100	0
2560	164	164	164	0
4096	100	100	100	0
8192	100	100	100	0
9472				
10000	0			
0	398788			
16384	100	100	100	0
65664	16	16	16	0

デバイスで上記のセキュリティ侵害の兆候が発生したお客様は、サポート部門に連絡して、この状態がこの脆弱性の不正利用に成功した結果であるかどうかを確認する必要があります。

## 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

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。

## 関連情報

最適な Cisco ASA、FTD、または FMC ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザーのガイダンスに従うことをお勧めします。

[Cisco ASA の互換性](#)

[Cisco Secure Firewall ASA アップグレードガイド](#)

[Cisco Secure Firewall Threat Defense 互換性ガイド](#)

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team ( PSIRT ) は、本アドバイザー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、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-intrusion-dos-DfT7wyGC>

## 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	2023年11月1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。