# Cisco 適応型セキュリティ仮想アプライアンスおよび Cisco Secure Firewall Threat Defense Virtual の SSL VPN におけるサービス妨害の脆弱性


アドバイザリーID : cisco-sa-asaftdvirtual-dos-MuenGnYR
CVE-2024-20260
初公開日 : 2024-10-23 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 : CSCwe44099 CSCwk12738

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仮想アプライアンス（ASAv）および Cisco Secure Firewall Threat Defense Virtual（FTDv）（旧称 Cisco Firepower Threat Defense Virtual）プラットフォームの VPN および管理 Web サーバーの脆弱性により、認証されていないリモート攻撃者が仮想デバイスのシステムメモリ不足を引き起こし、その結果 SSL VPN 接続の処理速度が低下して、最終的にすべての機能が停止する可能性があります。

この脆弱性は、仮想プラットフォームでの新規の着信 SSL/TLS 接続に対して、メモリ管理が適切に行われていないことに起因します。攻撃者は、大量の新しい着信 SSL/TLS 接続を標的の仮想プラットフォームに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスのシステムメモリを枯渇させ、サービス妨害（DoS）状態を引き起こす危険性があります。攻撃トラフィックが停止すると徐々にメモリを再利用できるようになりますが、速やかに動作を復旧させるには、手動でのリロードが必要になる場合があります。

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-asaftdvirtual-dos-MuenGnYR

このアドバイザリは、2024 年 10 月に公開された Cisco ASA、FMC、および FTD ソフトウェアのセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、『Cisco Event Response: October 2024 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

この脆弱性の影響を受けるのは、デバイスで SSL/TLS メッセージを処理する機能が設定されている Cisco ASAv および FTDv です。これらの機能には次のようなものがあります。

- SSL VPN
- 管理インターフェイスに使用される HTTP サーバ

注：仮想 Cisco ASA および FTD プラットフォーム以外はこの脆弱性の影響を受けません。

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。

## デバイスで SSL または TLS メッセージ処理の可能性があるかどうかの確認

Cisco ASAv または FTDv デバイスで SSL または TLS パケットが処理されるかどうかを確認するには、show asp table socket コマンドを使用します。 | include SSL|DTLS コマンドを使用して、コマンドの出力を確認します。このコマンドの出力が空の場合、デバイスは影響を受けません。以下の例で示すようにコマンドの何らかの出力が返される場合、デバイスは影響を受けます。

```
<#root>

asa#

show asp table socket | include SSL|DTLS


SSL        0005aa68  LISTEN     x.x.x.x:443      0.0.0.0:*
SSL        002d9e38  LISTEN     x.x.x.x:8443     0.0.0.0:*
DTLS       0018f7a8  LISTEN     10.0.0.250:443   0.0.0.0:*
```

注：仮想 Cisco ASA および FTD プラットフォーム以外はこの脆弱性の影響を受けません。

## 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。

- Cisco ASA または FTD ソフトウェアを実行しているハードウェアベースのプラットフォーム
- Cisco Secure Firewall Management Center（FMC）ソフトウェア（旧称 Firepower Management Center 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ます。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）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 | |

注：Cisco ASA ソフトウェアが実行されている Cisco 3000 シリーズ産業用セキュリティアプライアンス（ISA）については、Cisco ASA ソフトウェアのリリース 9.16.4.67 は見送られ、リリース 9.16.4.70 に置き換えられています。

## 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、そのアドバイザリ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、シスコ内部でセキュリティテストを実施中、シスコの Vivek Singh によって発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdvirtual-dos-MuenGnYR

## 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 10 月 23 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。