Cisco Secure Firewall Threat DefenseソフトウェアのTLS 1.3におけるDenial of Service(DoS)の脆弱性

Advisory ID : cisco-sa-ftd-tls1.3-dos-dLxwFWgF
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco Bug ID : CSCwo83926

CVE-2026-20135

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco Secure Firewall Threat Defense(FTD)ソフトウェアのTLS 1.3実装の脆弱性により、認証されていないリモートの攻撃者が該当デバイスの予期しない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、TLS 1.3接続中の不適切なバッファ管理に起因します。細工された TLS 1.3 パケットが、TLS 1.3 が有効なリスニングソケットを介して該当システムに送信されると、この脆弱性が不正利用され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LINAプロセスをクラッシュさせ、デバイスがリロードされる可能性があります。リロードは、接続の認証の前または後に発生する可能性があります。

注：TLS 1.3接続には、データトラフィックとユーザ管理トラフィックの両方が含まれます。

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-ftd-tls1.3-dos-dLxwFWgF

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、2026年9月16日発行のCisco Advance Notification, Security Advisoriesを参照してください。また、Cisco Secure Firewall製品の改善と修正に関するさらに詳しいドキュメントにつ

いては、『Cisco Secure Firewall Adaptive Security Appliance Software、Secure Firewall Threat Defense Software、およびSecure Firewall Management Centerソフトウェア強化リリース：2026年9月』を参照してください。

該当製品

脆弱性がある製品

この脆弱性は、Cisco Secure FTDソフトウェアの脆弱性が存在するリリースを実行し、TLS 1.3接続を許可するように設定されたSSLリスニングソケットを持つシスコデバイスに影響を与えます。

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。

デバイスが TLS パケットを処理できるかどうかの確認

Cisco Secure FTDソフトウェアを実行しているデバイスがTLSパケットを処理できるかどうかを確認するには、show asp table socket | include SSLコマンドを使用して、任意のTCPポートでSSLリスニングソケットを検索します。次の例は、TCPポート443および8443でのSSLリスニングソケットの出力を示しています。

```
<#root>

ftd#

show asp table socket | include SSL


SSL       00185038  LISTEN     172.16.0.250:

443

    0.0.0.0:*
SSL       00188638  LISTEN      10.0.0.250:

8443

    0.0.0.0:*
```

ソフトウェア設定でのTLSバージョンの確認

デバイスでCisco Secure FTDソフトウェアが実行されており、TLS 1.3が設定されているかどうかを確認するには、show running-config all ssl CLIコマンドを使用します。出力には、設定されている最大TLSバージョンが表示されます。次の例に示すように、見つかったバージョンがTLS 1.3である場合、デバイスはこの脆弱性の影響を受ける可能性があります。

```
<#root>
```

```
ftd# show running-config all ssl
ssl server-max-version tlsv1.3
```

Cisco Secure FTDソフトウェアでTLS 1.3の設定を確認するもう1つの方法は、Cisco Secure Firewall Management Center(FMC)ソフトウェアで次の手順を使用することです。

1. Cisco Secure FMCソフトウェアにログインします。
2. メニューバーからDevices > Platform Settingsの順に選択します。
3. 該当デバイスに適用するプラットフォーム設定ポリシーを追加または編集します。
4. 左側のナビゲーションメニューから、SSLを選択します。
5. TLS versionドロップダウンメニューから、TLSv1.3が選択されているかどうかを確認します。

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。

- Cisco Secure Firewall 適応型セキュリティアプライアンス（ASA）ソフトウェア
- Cisco Secure FMC 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、管理者がデバイスの設定からTLS 1.3を一時的に削除する場合があります。Cisco Secure FMCソフトウェアとFlexConfigオブジェクトを使用して、最小および最大のTLSバージョンをTLS 1.2に設定します。FlexConfigオブジェクトの詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「FTDのFlexConfigポリシー」の章を参照してください。

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、回避策や緩和策（該当する場合）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の一時的な解決策であると考えています。この脆弱性を修正し、本

アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載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 Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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、セキュリティへの影響の評価（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 Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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	

関連情報

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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 Secure Firewall 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 Cisco Cisco Technical Assistance Center（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-ftd-tls1.3-dos-dLxwFWgF

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	2026年9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center（TAC）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。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。