Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Cisco Secure Firewall Threat Defense の各ソフトウェアの SSL/TLS 証明書におけるサービス妨害（DoS）脆弱性

アドバイザリーID : cisco-sa-asaftd-ssltls-dos-eHw76vZe
CVE-2025-20134
初公開日 : 2025-08-14 16:00
最終更新日 : 2025-08-19 16:32
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwk44159

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 Secure Firewall 適応型セキュリティアプライアンス（ASA）ソフトウェアおよび Cisco Secure Firewall Threat Defense（FTD）ソフトウェアの 証明書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予期しない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。

この脆弱性は、SSL/TLS 証明書の不適切な解析に起因します。攻撃者は、DNS インスペクションが有効になっている静的なネットワークアドレス変換（NAT）ルールに一致するよう巧妙に細工された DNS パケットを該当デバイスを介して送信することにより、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-asaftd-ssltls-dos-eHw76vZe

このアドバイザリは、2025 年 8 月に公開された Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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: August 2025 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure 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、SSL/TLS リスニングソケットを備え、Cisco Secure Firewall ASA ソフトウェアリリース 9.15 以前または Cisco Secure FTD ソフトウェアリリース 6.7 以前を実行しているシスコデバイスに影響を与えます。

脆弱性のある Cisco ソフトウェアリリースの詳細については、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 SSL/TLS パケットを処理できるかどうかの確認

Cisco Secure Firewall ASA ソフトウェアまたは Cisco Secure FTD ソフトウェアを実行しているデバイスが SSL/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、すべての 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 SSL リスニングソケットを使用する Cisco Secure Firewall ASA デバイスの出力を示しています。

```
<#root>

ciscoasa#

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:*
```

次の表では、左の列に、通信に SSL/TLS を使用しているソフトウェア機能を記載しています。右の列は、show running-config CLI コマンドの各機能の基本設定を示しています。これらの機能により、SSL リスニングソケットが有効になる可能性があります。

ソフトウェア機能	脆弱性の可能性がある設定
有効な HTTP サーバー[1、2]	

ソフトウェア機能	脆弱性の可能性がある設定
	http server enable http <ip_address> <subnet_netmask> <interface_name>
SSL VPN[3]	webvpn enable <interface_name>

1. この機能は、設定されたアクセスホストの IP アドレスに対してのみ脆弱です。
2. Cisco Secure FTD ソフトウェアの場合、HTTP 機能は、Cisco Secure Firewall Management Center（FMC）コンソールで [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [HTTPアクセス（HTTP Access）] の順に選択すると有効になります。
3. Cisco Secure FTD ソフトウェアの場合、リモートアクセス VPN 機能は、Cisco Secure FMC ソフトウェアで [デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）] の順に選択するか、Cisco Secure Firewall Device Manager（FDM）で [リモートアクセス VPN（Remote Access VPN）] を選択すると有効になります。

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 Cisco Secure FMC ソフトウェアには影響を与え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完全なアップグレード ソリューション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。

修正済みリリース

次の表では、左の列に Cisco Secure Firewall ASA および Cisco Secure FTD の各ソフトウェアリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Secure Firewall ASA ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
9.15 以前	修正済みリリースに移行。
9.16 以降	脆弱性なし

Cisco Secure FTD ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
6.7 以前	修正済みリリースに移行。
7.0 以降	脆弱性なし

シスコの 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検証します。

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

Cisco Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC 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 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 PSIRT では、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は確認しておりません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の Jason Crowder による内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssltls-dos-eHw76vZe

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	影響を受けるデバイスに関する情報を明確化。	要約	Final	2025 年 8 月 19 日
1.0	初回公開リリース	—	Final	2025 年 8 月 14 日

利用規約

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。