Cisco Secure Firewall Threat DefenseソフトウェアのSnort 2におけるSSL/TLSに関するDoS脆弱性

Medium

Advisory ID : cisco-sa-ftd-snort2-ssldos-Mw7WYX9c
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco Bug ID : CSCwu03757

CVE-2026-20290

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Snort 2検出エンジンにおけるSSL/TLS証明書解析の脆弱性により、認証されていないリモートの攻撃者がSnort 2検出エンジンを再起動させる可能性があります。

この脆弱性は、SSL証明書の検証が不完全であることに起因します。攻撃者は、巧妙に細工されたSSL接続セットアップ要求を送信してSnort 2で解析することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はSnort 2検出エンジンを予期せず再起動させ、サービス拒否(DoS)状態を引き起こす可能性があります。

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-ftd-snort2-ssldos-Mw7WYX9c

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

公開時点でこの脆弱性の影響を受けた製品については、次のセクションを参照してください。

オープンソースの Snort 2

この脆弱性は、公開時点でオープンソースのSnort 2に影響を与えました。

公開時点で脆弱性が存在するSnort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。Snortの詳細については、Snort Webサイトを参照してください。

Cisco Secure FTDソフトウェア

公開時点で、Snort 2が設定されている場合、これらの脆弱性はCisco Secure FTDソフトウェアに影響を与えました。

脆弱性が存在するCisco Secure FTD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。

Cisco Secure FTD ソフトウェアの Snort 設定の確認

Cisco Secure FTDソフトウェアリリース7.0.0以降の新規インストールでは、Snort 3がデフォルトで実行されます。Cisco Secure FTDソフトウェアリリース6.7.0以前を実行していて、リリース7.0.0以降にアップグレードされたデバイスでは、デフォルトでSnort 2が実行されます。
Snort 2は、Cisco Secure FTDソフトウェアリリース7.7.0以降では廃止されました。

Cisco Secure FTDソフトウェアで実行されているSnortのバージョンを確認するには、「Firepower Threat Defense(FTD)で実行されるアクティブなSnortバージョンの確認」を参照してください。

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製品には影響を与えないことを確認しました。

- Cisco Cyber Vision
- Cisco Meraki MXセキュリティアプライアンス
- Cisco Secure Access Secure Internet Access(SIA)の利点
- Cisco Secure Access Secure Private Access(SPA)の利点
- 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 Firewall Management Center（FMC）ソフトウェア
- Cisco Umbrella Cloud-delivered Firewall(CDFW)(旧称Umbrella Secure Internet Gateway(SIG))
- オープンソースの Snort 3
- Cisco IOS XEソフトウェア向けUnified Threat Defense(UTD)Snort IPS Engine
- Cisco IOS XE SD-WANソフトウェア用UTDエンジン

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。

修正済みリリース

修正済みリリースの詳細については、次の項を参照してください。

オープンソースの Snort 2

シスコはオープンソースSnort 2を公式に廃止し、サポート終了を迎えました。最後のオープンソースSnort 2リリースは2.9.20です。この製品のサポート終了通知を参照することをお勧めします。

Snort 2のバージョンのサポート終了のお知らせ

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 FTDソフトウェアリリースの判別に関するサポートについては、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 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-snort2-ssldos-Mw7WYX9c

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。