Snort 3検出エンジンを使用したCisco Secure Firewall Threat DefenseソフトウェアのTLSにおけるサービス妨害の脆弱性

Medium

アドバイザリーID : cisco-sa-ftd-tcp-dos-rHfqnwRg
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwn73801

CVE-2026-20006

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 Threat Defense(FTD)ソフトウェアのSnort 3検出エンジンのTLS暗号化機能の脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを予期せず再起動させ、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プロトコルの不適切な実装に起因します。攻撃者は、巧妙に細工されたTLSパケットを該当システムに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。エクスプロイトに成功すると、攻撃者はCisco Secure FTDソフトウェアを実行しているデバイスでネットワークトラフィックをドロップさせ、DoS状態を引き起こす可能性があります。

注：TLS 1.3はこの脆弱性の影響を受けません。

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。本脆弱性に対処する回避策がいくつかあります。

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-tcp-dos-rHfqnwRg

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアセキュリティアドバイザリバンドル』の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 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

公開時点で、この脆弱性の影響を受けたシスコ製品では、脆弱性が存在するCisco Secure FTDソフトウェアまたはCisco FirePOWER Servicesのリリースを実行していて、次の条件を満たしている必要があります。

- Snort 3が有効になりました。
- SSLまたは暗号化解除ポリシーが、特定のTLSバージョンからのトラフィックをブロックするルールと共に展開されました。
- SSLまたは暗号化解除ポリシーが、サポートされていない暗号のトラフィックを暗号化解除しないように設定されています。

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。

Cisco Secure FTD ソフトウェアの Snort 設定の確認

Cisco Secure FTD ソフトウェアで Snort 3 が実行されているかどうかを確認するには、「Firepower Threat Defense（FTD）で実行されているアクティブな Snort バージョンの判別」を参照してください。 この脆弱性がエクスプロイトされるのは、Snort 3 がアクティブである場合に限ります。

Cisco Secure FTDソフトウェアのSSLまたは復号化ポリシー設定の確認

Cisco Secure Firewall Management Center(FMC)ソフトウェアで管理されているデバイスにSSLまたは復号化ポリシーが設定されているかどうかを確認するには、次の手順を使用します。

1. Cisco Secure FMCソフトウェアのWebベース管理インターフェイスにログインします。
2. Policiesメニューから、Access Control > SSLまたはAccess Control > Decryptionを選択します。
    - ポリシーがリストされていない場合、デバイスはこの脆弱性の影響を受けません。
    - ポリシー名がリストされている場合、デバイスにはSSLまたは復号化ポリシーが適用されており、この脆弱性の影響を受ける可能性があります。次の設定チェックに進みます。

Cisco Secure FTDソフトウェアのSSLまたは復号化ポリシー設定が特定のTLSバージョンからのトラフィックをブロックしているかどうかを確認する

前のセクションで特定されたSSLまたは復号化ポリシーが、特定のTLSバージョンからのトラ

フィックをブロックするかどうかを確認するには、次の手順を使用します。

1. Cisco Secure FMCソフトウェアのWebベース管理インターフェイスにログインします。
2. Policiesメニューから、Access Control > SSLまたはAccess Control > Decryptionの順に選択します。
3. 適切なSSLまたは復号化ポリシーを選択します。
4. 編集鉛筆アイコンをクリックします。
5. 適切なルールを選択します。
6. 編集鉛筆アイコンをクリックします。
7. Version タブをクリックします。
    - すべてのチェックボックスをオンにしても、デバイスはこの脆弱性の影響を受けません。
    - TLS v1.0、TLS v1.1、またはTLS v1.2のチェックマークが外れていて、アクションがブロックされている場合、デバイスは特定のTLSバージョンからのトラフィックをブロックするため、この脆弱性の影響を受ける可能性があります。次の設定チェックに進みます。

Cisco Secure FTDソフトウェアのSSLまたは復号化ポリシー設定が、サポートされていない暗号のトラフィックを復号化するかどうかを確認する

SSLまたは復号化ポリシーが、サポートされていない暗号のトラフィックを復号化しないように設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Secure FMCソフトウェアのWebベース管理インターフェイスにログインします。
2. Policiesメニューから、Access Control > SSLまたはAccess Control > Decryptionを選択します。
3. 適切なSSLまたは復号化ポリシーを選択します。
4. 編集鉛筆アイコンをクリックします。
5. Undecryptable Actions タブをクリックします。
    - Unsupported Cipher SuiteがDo not decryptの場合、デバイスはこの脆弱性の影響を受けます。
    - Unsupported Cipher SuiteがInherit Default Actionで、Default ActionがDo not decryptの場合、デバイスはこの脆弱性の影響を受けます。
    - Unsupported Cipher SuiteがInherit Default Actionで、Default ActionがBlock または Block with resetの場合、デバイスはこの脆弱性の影響を受けません。
    - Unsupported Cipher SuiteがDo not decryptまたはInherit Default Actionでない場合、デバイスはこの脆弱性の影響を受けません。

Cisco Secure FTDソフトウェアのSSLまたは復号化ポリシーのデフォルトのアク

ション設定の確認

SSLまたは復号化ポリシーのデフォルトアクションを確認するには、次の手順に従います。

1. Cisco Secure FMCソフトウェアのWebベース管理インターフェイスにログインします。
2. Policiesメニューから、Access Control > SSLまたはAccess Control > Decryptionを選択します。
3. 適切なSSLまたは復号化ポリシーを選択します。
4. 編集鉛筆アイコンをクリックします。
5. Rulesタブをクリックします。
6. デフォルトアクションを表示します。

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製品には影響を与えないことを確認しました。

- シスコセキュアアクセス
- 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
- Cisco Cyber Vision
- Cisco Meraki 製品
- Cisco Secure Access - Secure Internet Access(SIA)の利点
- シスコセキュアアクセス – セキュアプライベートアクセス(SPA)の利点
- Cisco Umbrella Cloud-delivered Firewall(CDFW)(旧称Umbrella Secure Internet Gateway(SIG))
- Cisco Unified Threat Defense(UTD)
- オープンソースの Snort 2
- オープンソースの Snort 3

回避策

この脆弱性の回避策として、特定のTLSバージョンからのトラフィックがブロックされないようにデバイスを設定します。回避策を実装するには、次の手順に従います。

1. Cisco Secure FMCソフトウェアのWebベース管理インターフェイスにログインします。
2. Policiesメニューから、Access Control > SSLまたはAccess Control > Decryptionを選択します。
3. 適切なSSLまたは復号化ポリシーを選択します。
4. 編集鉛筆アイコンをクリックします。

5. 適切なルールを選択します。
6. 編集鉛筆アイコンをクリックします。
7. Version タブをクリックします。
8. すべてのバージョンのチェックボックスがオンになっていることを確認します。
9. Saveをクリックして、変更を展開します。

この回避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。この脆弱性を完全に修正し、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

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 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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-rHfqnwRg

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3月4日

利用規約

本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、

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。