Cisco Secure Firewall Threat DefenseソフトウェアのSnort 3 SSLメモリ管理におけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-ftd-snort3ssl-FBEKYXpH
CVE-2026-20052
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 : No workarounds available
Cisco バグ ID : CSCwn63410

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検出エンジンにおけるメモリ管理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によってSnort 3検出エンジンが再起動させられる可能性があります。

この脆弱性は、デバイスがSnort 3 SSLパケットインスペクションを実行しているときにメモリ管理の論理エラーが発生することに起因します。攻撃者は、確立された接続を介して巧妙に細工されたSSLパケットを送信し、Snort 3検出エンジンによって解析されることで、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、Snort 3検出エンジンが予期せず再起動したときに、サービス拒否(DoS)状態が引き起こされる危険性があります。

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-snort3ssl-FBEKYXpH

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、シスコデバイスが脆弱性のあるCisco Secure FTDソフトウェアリリースを実行しており、次の条件を満たしている場合、この脆弱性の影響を受けました。

- Snort 3が有効になりました。
- SSLポリシーが設定されました。

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ポリシー設定の確認

SSL復号化ポリシーはデフォルトでは設定されていません。

CLIを使用したCisco Secure FTDソフトウェアのSSLポリシー設定の確認

Cisco Secure FTDソフトウェアを実行しているデバイスでSSLポリシーが設定されているかどうかを確認するには、Cisco Secure FTDソフトウェアのCLIにログインし、show ssl-policy-configコマンドを使用します。コマンド出力にポリシーが示されている場合、デバイスにはSSLポリシーが適用されており、次の例に示すとおり、この脆弱性の影響を受けます。

```
<#root>

>

show ssl-policy-config


=================[ Default Action ]=================
Default Action             : Do Not Decrypt
...
```

次の例では、SSLポリシーは適用されていません。

```
<#root>
```

```
>
show ssl-policy-config

SSL policy not yet applied
```

Cisco Secure FDMソフトウェアで管理されるデバイスのCisco Secure FTDソフトウェアSSLポリシー設定の確認

Cisco Secure Firepower Device Manager(FDM)ソフトウェアで管理されているデバイスにSSLポリシーが設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Secure FTDのWebインターフェイスにログインします。
2. メインメニューから、Policiesを選択します。
3. SSL Decryptionタブを選択します。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - SSL復号化が有効になっていない場合、デバイスはこの脆弱性の影響を受けません。

SSL復号化ポリシーの詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「SSL Decryption」の章を参照してください。

Cisco Secure FMCソフトウェアで管理されているデバイスのCisco Secure FTDソフトウェアSSL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、次の手順を実行します。

1. Cisco Secure FMC Web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を選択します。
3. 適切なアクセスコントロールポリシーを選択します。
4. Edit鉛筆アイコンをクリックします。
5. SSL Policy領域を調べます。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - Noneが表示される場合、そのデバイスはこの脆弱性の影響を受けません。

SSL復号化ポリシーの詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』の「SSL Policies」の章を参照してください。

Cisco Defense Orchestratorで管理されるデバイスのCisco FTDソフトウェアSSLポリシー設定の確認

Cisco Defense Orchestratorで管理されているデバイスにSSLポリシーが設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Policiesメニューから、FTD Policiesを選択します。
3. FTD Policiesメニューから、Access Controlを選択します。
4. 適切なアクセスコントロールポリシーを選択します。
5. Edit鉛筆アイコンをクリックします。
6. Decryption Policy領域を調べます。
    - Policy Nameがリストされている場合、デバイスはこの脆弱性の影響を受けます。
    - Noneが表示される場合、そのデバイスはこの脆弱性の影響を受けません。

Cisco Defense Orchestratorで管理されるデバイスの詳細については、Cisco Defense Orchestratorのドキュメント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 ソフトウェア
- 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 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
- Snort 2が設定されたCisco Secure FTDソフトウェア
- Cisco Umbrella Cloud-delivered Firewall(CDFW)(旧称Umbrella Secure Internet Gateway(SIG))
- Cisco Unified Threat Defense（UTD）ソフトウェア
- オープンソース Snort 2 ソフトウェア
- オープンソース Snort 3 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

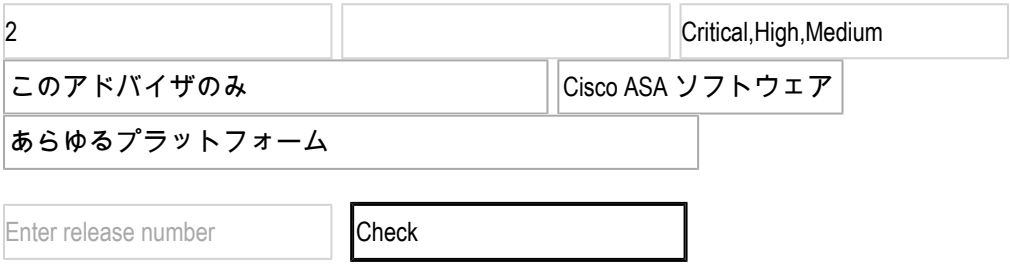
シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。



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

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-snort3ssl-FBEKYXpH

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

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。