

Cisco Firepower Threat Defense ソフトウェアの Snort メモリ不足によるサービス妨害の脆弱性



アドバイザリーID : cisco-sa-ftd-snort-dos- [CVE-2022-20751](#)
hd2hFgM

初公開日 : 2022-04-27 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvu41615](#)

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 Firepower Threat Defense (FTD) ソフトウェアの Snort 検出エンジン統合における脆弱性により、認証されていないリモートの攻撃者が該当デバイスで無制限のメモリ消費を引き起こし、サービス妨害状態 (DoS) が発生する可能性があります。

この脆弱性は、特定の Snort イベントに関するメモリ管理が不十分であることに起因します。攻撃者は、該当デバイスで特定の Snort イベントを生成するように細工された一連の IP パケットを該当デバイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。持続的な攻撃により、該当デバイスでメモリ不足状態が引き起こされる可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスを通してすべてのトラフィックを中断させる可能性があります。状況によっては、該当デバイスのリロードが引き起こされ、DoS 状態にな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。

このアドバイザリーは、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-snort-dos-hd2hFgM>

このアドバイザリーは、2022 年 4 月に公開された Cisco ASA、FTD、および FMC のセキュリティアドバイザリーバンドルに含まれています。アドバイザリーとリンクの一覧については、[Cisco Event Response : 2022 年 4 月に公開された Cisco ASA、FMC、および FTD ソフトウェア セキュリティアドバイザリーバンドル](#) を参照してください。

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、次のシスコ製品で、脆弱性が存在する Cisco FTD ソフトウェアリリースを実行し、接続ロギングが有効になっている場合です。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ

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。

脆弱性を含ま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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#)

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。

- 1000 シリーズ サービス統合型ルータ (ISR)
- 3000 シリーズ産業用セキュリティ アプライアンス (ISA)
- 4000 シリーズ ISR
- 適応型セキュリティ アプライアンス (ASA) ソフトウェア
- ASA 5500-X with FirePOWER Services
- Cloud Services Router (CSR) 1000V シリーズ
- Firepower 9300 シリーズ
- Firepower Management Center (FMC) ソフトウェア
- Firepower NGFW 仮想 (NGFWv)
- サービス統合型仮想ルータ (ISRv)
- Meraki MX セキュリティ アプライアンス
- オープンソースの Snort 2 検出エンジン
- オープンソースの Snort 3 検出エンジン

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ン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です。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 [Cisco Support and Downloads 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。

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、左の列にシスコソフトウェアのリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、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。右側の列は、リリースがこのバンドルに記載された「重大」または「高」SIR 脆弱性のいずれかに該当するかどうか、およびそれらの脆弱性に対する修正を含むリリースを示しています。

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
6.2.2 以前 ¹	修正済みリリースに移行。	修正済みリリースに移行。
6.2.3	修正済みリリースに移行。	修正済みリリースに移行。
6.3.0 ¹	修正済みリリースに移行。	修正済みリリースに移行。
6.4.0	6.4.0.15 (May 2022)	6.4.0.15 (May 2022)
6.5.01	修正済みリリースに移行。	修正済みリリースに移行。
6.6.0	6.6.3	6.6.5.2
6.7.0	修正済みリリースに移行。	修正済みリリースに移行。
7.0	脆弱性なし	7.0.2 (May 2022)
7.1	脆弱性なし	7.1.0.1

1. Cisco FMC および FTD ソフトウェアリリース 6.2.2 以前および 6.3.0、6.5.0 については、[ソフトウェアのメンテナンスが終了](#)しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

FTD デバイスのアップグレード手順については、[Cisco Firepower Management Center アップグレードガイド](#)を参照してください。

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されたリリース情報のみを検証します。

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、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fts-snort->

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	2022 年 4 月 27 日

利用規約

本アドバイザー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。本アドバイザー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。

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