Cisco Secure Firewall適応型セキュリティアプライアンスソフトウェアのTCPフラッドによるサービス妨害(DoS)の脆弱性

アドバイザリーID : cisco-sa-asa-dos-FCvLD6vR
初公開日 : 2026-03-04 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 : CSCwr58661

CVE-2026-20082

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)ソフトウェアの初期接続制限の処理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着信TCP SYNパケットを誤ってドロップする可能性があります。

この脆弱性は、デバイスがTCP SYNフラッド攻撃を受けている場合に、管理インターフェイスまたはデータインターフェイスを宛先とする新しい着信TCP接続が不適切に処理されることに起因します。攻撃者は、巧妙に細工されたトラフィックストリームを該当デバイス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、リモート管理アクセス、リモートアクセスVPN(RAVPN)接続、およびTCPベースのすべてのネットワークプロトコルを含む、デバイスへのすべての着信TCP接続の確立を阻止できる可能性があります。これにより、影響を受ける機能に対してサービス拒否(DoS)状態が発生します。

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-asa-dos-FCvLD6vR

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

この脆弱性は、デバイス設定に関係なく、Cisco Secure Firewall ASAソフトウェアリリース9.20.4.14にのみ影響を与えます。この脆弱性の修正済みソフトウェアリリースは、Cisco Secure Firewall ASAソフトウェアリリース9.20.4.19です。

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。

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 Firewall Management Center(FMC)ソフトウェアまたはCisco Secure Firewall Threat Defense(FTD)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。

修正済みリリース

次の表に示すように、該当する修正済みのソフトウェア 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）
9.20.4.14	9.20.4.19

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。

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 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-asa-dos-FCvLD6vR

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

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。