

Cisco Secure Firewall 適応型セキュリティアプライアンスおよびSecure Firewall Threat DefenseソフトウェアのVPN Webサービスクライアント側の要求密輸の脆弱性



アドバイザリーID : cisco-sa-asaftd-desync-[CVE-2026-n5AVzEQw](#) [20069](#)

初公開日 : 2026-03-04 16:00

バージョン 1.0 : Final

CVSSスコア : [4.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwq02055](#)

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 Adaptive Security Appliance(ASA)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアのVPN Webサービスコンポーネントの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのユーザに対してブラウザベースの攻撃を行う可能性があります。

この脆弱性は、HTTP要求の不適切な検証に起因します。攻撃者は、Cisco Secure Firewall ASAソフトウェアまたはCisco Secure FTDソフトウェアを実行していて、VPN機能をサポートするWebサービスエンドポイントが有効になっているデバイスに、悪意のあるHTTP要求を渡すように設計されているWebサイトにユーザを誘導することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスから使用中のブラウザに悪意のある入力を反映させ、クロスサイトスクリプティング(XSS)攻撃を含むブラウザベースの攻撃を実行できる可能性があります。攻撃者は、影響を受けるデバイスに直接影響を与えることはできません。

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。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-asaftd-desync-n5AVzEQw>

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

この脆弱性の公開時点では、次の機能のいずれかまたは両方が設定されたCisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアの脆弱性が存在するリリースを実行するシスコ製品に、この脆弱性の影響が及んでいました。

- クライアントサービスを使用したインターネットキーエクスチェンジバージョン2(IKEv2)リモートアクセスVPN
- SSL VPN

注：リモートアクセスVPNサービスが、IKEv2リモートアクセスVPNのみを受け入れるように設定されていて、IKEv2クライアントサービスが無効になっているデバイスは、この脆弱性の影響を受けません。

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。

デバイス設定の確認

脆弱性のある機能がソフトウェアで有効になっているかどうかを確認するには、show running-config CLIコマンドを使用します。次の表では、左の列に、脆弱性が存在するCisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアの機能を示します。右の列は、show running-config CLI コマンドの各機能の基本設定を示しています。デバイスが脆弱なリリースを実行しており、これらの機能のいずれかが有効になっている場合、そのデバイスは脆弱であると見なされます。

Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェア機能	脆弱性の存在するコンフィギュレーション
IKEv2リモートアクセスVPN (クライアントサービスあり) ¹	crypto ikev2 enable client-services port
SSL VPN ¹	webvpn enable

Cisco Secure Firewall ASAソフトウェアまたは Secure FTDソフトウェア機能	脆弱性の存在するコンフィギュレーション

1. Cisco Secure FTDソフトウェアでは、Cisco Secure Firewall Management Center(FMC)ソフトウェアの Devices > VPN > Remote Access、またはCisco Secure Firewall Device Manager(FDM)の Remote Access VPNから、リモートアクセスVPN機能を有効にします。

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 Cisco Secure FMC 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。

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 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 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

この脆弱性を報告していただいたNetSPIのJosh Weber氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-desync-n5AVzEQw>

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。