Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Cisco Secure Firewall Threat Defense の各ソフトウェアのリモートアクセス SSL VPN におけるサービス妨害（DoS）脆弱性

アドバイザリーID : cisco-sa-asaftd-vpn-m9sx6MbC
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 : CSCwo49934 CSCwo49932 CSCwo73889 CSCwo73886 CSCwo73891

CVE-2026-20105
CVE-2026-20106
CVE-2026-20103
CVE-2026-20101
CVE-2026-20100

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)ソフトウェアのリモートアクセスSSL VPN機能における複数の脆弱性により、リモート攻撃者が該当デバイスの応答を停止させたり、予期せぬリロードを引き起こしたりする可能性があります。その結果、サービス妨害(DoS)状態が発生し、手動でのリブートが必要になることがあります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-asaftd-vpn-m9sx6MbC

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

これらの脆弱性は、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しており、クライアントサービスまたはリモートアクセスSSL VPN機能を備え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が有効になっているシスコデバイスに影響を与えます。CVE-2026-20106は、管理HTTPサーバ(MS)およびMobile User Security(MUS)機能が有効になっている場合は、これらの機能にも影響を与えます。各製品の脆弱な状態については、次の表を参照してください。

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 Firewall ASA ソフトウェアにおける脆弱性のある設定

次の表では、左列に潜在的脆弱性のある Cisco Secure Firewall ASA ソフトウェアの機能を記載しています。右列に示す Cisco ASA 機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。これらの機能により、SSLリスニングソケットが有効になる可能性があります。

Cisco Secure Firewall ASA ソフトウェアの機能	脆弱性の可能性がある設定
IKEv2リモートアクセスVPN（クライアントサービス付き）	`crypto ikev2 enable <interface name> client-services port <port_numbers>`
管理 Web サーバーアクセス（Cisco Adaptive Security Device Manager（ASDM）および Cisco Security Manager アクセスを含む）[1]	`http server enable` `http`

Cisco Secure Firewall ASA ソフトウェアの機能	脆弱性の可能性がある設定
モバイル ユーザ セキュリティ（MUS）	webvpn mus password mus server enable <*port_number*> mus <*IPv4_address*> <*IPv4_mask*> <*interface_name*>
SSL VPN	webvpn enable <*interface_name*>

1. この機能は、設定されたアクセスホストに含まれるIPアドレスに対してのみ脆弱です。

Cisco Secure FTDソフトウェアの脆弱な設定

次の表では、左列に潜在的脆弱性のある Cisco Secure Firewall FTD ソフトウェアの機能を記載しています。右列に示す Cisco ASA 機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。これらの機能により、SSLリスニングソケットが有効になる可能性があります。

Cisco Secure FTD ソフトウェアの機能	脆弱性の可能性がある設定
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 <*interface_name*> client-services port <*port_numbers*>
SSL VPN[1]	webvpn enable <*interface_name*>
HTTP サーバーが有効[2、3]	http server enable http

Cisco Secure FTD ソフトウェアの機能	脆弱性の可能性がある設定

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。
2. Cisco Secure FTDソフトウェアの場合、HTTP機能はCisco Secure FMCコンソールの Devices > Platform Settings > HTTP Accessで有効になっています。
3. この機能は、設定されたアクセスホストに含まれるIPアドレスに対してのみ脆弱です。

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」セクションに記載されている製品のみが、これら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、これらの脆弱性が 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。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20101:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN認証のDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN(SSL VPN)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デバイスの予期しないリロードを引き起こし、その結果DoS状態が発生する可能性があります。

この脆弱性は、VPN認証メッセージを処理する際の不十分なエラーチェックに起因します。攻撃者は、巧妙に細工されたメッセージをVPN認証サービ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。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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。

バグID: CSCwo49932
CVE ID：CVE-2026-20101
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.6
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20103:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPNメモリ枯渇のDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN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デバイスメモリを枯渇させ、新しいリモートアクセスSSL VPN接続にDoSが発生する可能性があります。この脆弱性により、管理インターフェイスが一時的に応答しなくなる可能性があります。

この脆弱性は、ユーザー入力の検証が不十分なことに起因します。攻撃者は、巧妙に細工されたパケットをリモートアクセスSSL VPNサーバ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、攻撃者は該当デバイスのWebインターフェイスの応答を停止させ、DoS状態を引き起こす可能性があります。

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。

バグID: CSCwo49934
CVE ID：CVE-2026-20103
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.6
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20100:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN LuaインタープリタのDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN機能のLuaインタープリタにおける脆弱性により、有効なVPNクレデンシャルを持つ認証されたリモートの攻撃者が、デバイスの予期せぬリロードを引き起こし、その結果DoS状態が発生する可能性があります。

この脆弱性は、Luaインタープリタへのユーザ入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたHTTPパケットをリモートアクセスSSL VPNサーバ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。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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。

バグID: CSCwo73889
CVE ID：CVE-2026-20100
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.7
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20105:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN認証メモリ枯渇のDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN(SSL VPN)機能の脆弱性により、有効なVPNクレデンシャルを持つ認証されたリモートの攻撃者がデバイスメモリを枯渇させ、結果としてサービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、ユーザー入力の検証が不十分なことに起因します。攻撃者は、巧妙に細工されたパケットをリモートアクセスSSL VPNサーバ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。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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。

バグID: CSCwo73891
CVE ID：CVE-2026-20105
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.7
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20106:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPNの非認証メモリ枯渇のDoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのリモートアクセスSSL VPN、HTTP管理、およびMUS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デバイスメモリを枯渇させ、DoS状態が発生して手動でのリブートが必要になる可能性があります。

この脆弱性は、ユーザー入力の検証が不十分なことに起因します。攻撃者は、巧妙に細工されたパケットをリモートアクセスSSL VPNサーバ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、該当デバイスの応答を停止させることが可能になり、その結果 DoS 状態が発生す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。

バグID: CSCwo73886
CVE ID：CVE-2026-20106
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

回避策

これら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。これら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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

CVE-2026-20100:この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKeane O'Kelleyによる内部セキュリティテストで発見されました。

CVE-2026-20101：この脆弱性は、Cisco ASIGのKyle Ossingerによる内部セキュリティテストで発見されました。

CVE-2026-20103：この脆弱性は、Alex LumsdenとCisco ASIGのJason Crowderによる内部セキュリティテストで発見されました。

CVE-2026-20105およびCVE-2026-20106：これらの脆弱性は、Cisco ASIGのJason Crowderによる内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC

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。