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ソフトウェアのリモートアクセス SSL VPNにおけるDoS脆弱性

アドバイザリーID : cisco-sa-asaftd-vpn-dos-dzv4mQFF
初公開日 : 2026-08-11 16:39
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwv96220

CVE-2026-20349

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サービスの脆弱性により、認証されていないリモートの攻撃者がデバイスの予期せぬリロードを引き起こし、その結果、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、HTTP要求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、該当デバイスのリモートアクセスSSL VPNサービスに巧妙に細工されたHTTP要求を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。

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-dos-dzv4mQFF

該当製品

脆弱性のある製品

この脆弱性は、Cisco Secure Firewall ASAソフトウェアまたはCisco 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、かつ次の表に示す1つ以上の脆弱性が存在するシスコデバイスに影響を与えます。

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およびFTDソフトウェアの脆弱な設定

次の表では、左の列に、脆弱性が存在する可能性のあるCisco Secure Firewall ASAおよびSecure FTDソフトウェアの機能を示します。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およびFTDソフトウェア機能	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を使用）[1]	`crypto ikev2 enable <interface_name> client-services port <port_numbers>`
SSL VPN[1]	`webvpn` ` enable <interface_name>`
ゼロトラストネットワークアクセス[2]	`zero-trust` ` enable`

1. Cisco Secure FTD ソフトウェアの場合、リモートアクセス VPN 機能は、 Cisco Secure Firewall Management Center （FMC）ソフトウェアの [デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）] または Cisco Secure Firewall Device Manager（FDM）の [リモートアクセスVPN（Remote Access VPN）] から有効にすることができます。
2. この機能は、Cisco Secure FTDソフトウェアでのみ使用できます。

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 Firewall Management Center（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ホットフィックス

シスコは、この脆弱性に対処するために次のホットフィックスをリリースしました。これらのホットフィックスを Cisco.com の Software Center からダウンロードできます。

Cisco Secure Firewall ASA ソフトウェアリリース	ホットフィックス名
9.161	89.16.4.50
9.181	89.18.4.50
9.20	9.20.4.235
9.22	9.22.3.191
9.23	9.23.1.211
9.24	9.24.1.221

1. 89で始まるホットフィックスをインストールする場合、ASDMリリース7.24.1.374をインストールします。これは、ASDMの以前のリリースではこのASAソフトウェアリリースの番号形式が認識されないためです。

Cisco Secure FTD ホットフィックス

Cisco Secure FTD ソフトウェアリリース	ホットフィックス名
7.0	Cisco_FTD_Hotfix_GC-7.0.9.1-1.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_GC-7.0.9.1-1.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_GC-7.0.9.1-1.sh.RE L.tar Cisco_FTD_SSP_Hotfix_GC-7.0.9.1-1.sh.RE L.tar
7.2	Cisco_FTD_Hotfix_HM-7.2.11.1-2.sh.RE L.tar

Cisco Secure FTD ソフトウェアリリース	ホットフィックス名
	Cisco_FTD_SSP_FP1K_Hotfix_HM-7.2.11.1-2.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_HM-7.2.11.1-2.sh.REL.tar Cisco_FTD_SSP_FP3K_Hotfix_HM-7.2.11.1-2.sh.REL.tar Cisco_FTD_SSP_Hotfix_HM-7.2.11.1-2.sh.RE L.tar
7.4	Cisco_FTD_Hotfix_HK-7.4.7.1-1.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_HK-7.4.7.1-1.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_HK-7.4.7.1-1.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_HK-7.4.7.1-1.sh.RE L.tar Cisco_FTD_SSP_Hotfix_HK-7.4.7.1-1.sh.RE L.tar Cisco_Secure_FW_TD_4200_Hotfix_HK-7.4.7.1-1.sh.REL.tar
7.6	Cisco_FTD_Hotfix_DD-7.6.4.1-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_DD-7.6.4.1-2.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_DD-7.6.4.1-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_DD-7.6.4.1-2.sh.RE L.tar Cisco_Secure_FW_TD_4200_Hotfix_DD-7.6.4.1-2.sh.REL.tar
7.7	Cisco_FTD_Hotfix_AN-7.7.11.1-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_AN-7.7.11.1-2.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_AN-7.7.11.1-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_AN-7.7.11.1-2.sh.RE L.tar Cisco_Secure_FW_TD_1200_Hotfix_AN-7.7.11.1-2.sh.REL.tar Cisco_Secure_FW_TD_4200_Hotfix_AN-7.7.11.1-2.sh.REL.tar
10.0	Cisco_FTD_Hotfix_S-10.0.0.1-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_S-10.0.0.1-2.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_S-10.0.0.1-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_S-10.0.0.1-2.sh.RE L.tar Cisco_Secure_FW_TD_200_Hotfix_R-10.0.0.1-2.sh.REL.tar Cisco_Secure_FW_TD_1200_Hotfix_S-10.0.0.1-2.sh.REL.tar Cisco_Secure_FW_TD_4200_Hotfix_S-10.0.0.1-2.sh.REL.tar Cisco_Secure_FW_TD_6100_Hotfix_S-10.0.0.1-2.sh.RE

Cisco Secure FTD ソフトウェアリリース	ホットフィックス名
	L.tar

注：Cisco Secure FTDデバイスのアップグレード手順については、該当する『Cisco Secure FMC upgrade guide』を参照してください。

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

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

2026年8月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性が活発に悪用されていることを認識しました。この脆弱性が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強くお勧めします。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。また、Valerio Brussani - @val_brux(harmonyguard.cloud)からもシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF

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8月11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。