

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IKEv2証明書認証におけるDoS脆弱性



Advisory ID : cisco-sa-asaftd-ikev2cert-dos- [CVE-2026-20249](#)
uWyc2xtv

初公開日 : 2026-09-16 16:00

最終更新日 : 2026-09-18 15:50

バージョン 1.1 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwt42671](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

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)ソフトウェアのインターネットキーエクスチェンジバージョン2(IKEv2)の証明書認証機能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によって該当デバイスの予期せぬリロードが引き起こされる可能性があります。

この脆弱性は、IKEv2接続セットアップの証明書認証フェーズ中の論理エラーに起因します。攻撃者は、巧妙に細工された証明書を使用してIKEv2 VPN接続の確立を試みることで、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IKEv2プロセスをクラッシュさせ、サービス拒否(DoS)状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-ikev2cert-dos-uWyc2xtv>

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、[2026年9月16日発行のCisco Advance Notification, Security Advisories](#)を参照してください。また、Cisco Secure Firewall製品の改善と修正に関するさらに詳しいドキュメントにつ

いては、『[Cisco Secure Firewall Adaptive Security Appliance Software、Secure Firewall Threat Defense Software、およびSecure Firewall Management Centerソフトウェア強化リリース : 2026年9月](#)』を参照してください。

該当製品

脆弱性がある製品

この脆弱性は、証明書認証でIKEv2 VPN機能が有効になっているCisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアに影響を与えます。

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。

ソフトウェア設定の判断

Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアでIKEv2が有効になっているかどうかを確認するには、show running-config crypto ikev2 | include enable CLIコマンドを使用します。このコマンドが出力を返す場合は、IKEv2 が 1 つ以上のインターフェイスで有効になっています。次の例は、outsideインターフェイスでIKEv2が有効になっているデバイスでの出力を示しています。

```
<#root>

firewall#
show running-config crypto ikev2 | include enable

crypto ikev2 enable
    outside client-services port 443
```

コマンドで空の出力が返された場合、そのデバイスはこの脆弱性の影響を受けません。

Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアでIKEv2が証明書認証用に設定されているかどうかを確認するには、次の例に示すように、show running-config crypto ikev2 | include trust CLIコマンドを使用します。

```
<#root>

firewall#
show running-config crypto ikev2 | include trust

crypto ikev2 remote-access
```

コマンドで空の出力が返された場合、そのデバイスはこの脆弱性の影響を受けません。

IKEv2が有効でトラストポイント証明書が設定されている場合、デバイスはこの脆弱性の影響を受けます。

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[脆弱性が存在する製品](#)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。

修正リリース

次の表では、左の列にシスコソフトウェアリリースを記載しています。中央の列には、このアドバイザリで説明されている脆弱性の影響を受けるホットフィックスを、右側の列にはこれらの脆弱性に対する修正が含まれる最初のソフトウェアリリースを示します。上記のホットフィックスリリースのいずれかをインストールしたお客様は、上記の最初の修正リリースをインストールする必要があります。

Cisco Secure Firewall ASA ソフトウェアリリース	該当するホットフィックスリリース	第 1 修正済みリリース
9.16 以前	N/A	9.16.4.103
9.18	9.18.4.135	9.18.4.94
9.20	9.20.4.235	9.20.4.49
9.22	9.22.3.191	9.22.3.26
9.23	9.23.1.195	9.23.1.47

Cisco Secure Firewall ASA ソフトウェアリリース	該当するホットフィックスリリース	第 1 修正済みリリース
	9.23.1.211	
9.24	9.24.1.155 9.24.1.221	9.24.1.26

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれら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。

Cisco Secure FTDソフトウェアリリースおよびSecure FMCソフトウェアリリース	第 1 修正済みリリース
7.0 以前	7.0.10
7.2	7.2.12
7.4	7.4.8
7.6	7.6.6
7.7	7.7.13
10.0	10.0.2
10.1	10.1.0

複数の脆弱性に対する修正が含まれているため、上記の表の最初の修正済み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。詳細は、『[Cisco Secure Firewall適応型セキュリティアプライアンス、Secure Firewall Threat Defense、およびSecure Firewall Management Centerソフトウェアの強化リリース：2026年9月](#)』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	

その他のリソース

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新しいリリースが推奨される場合、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-asaftd-ikev2cert-dos-uWyc2xtv>

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	修正済みリリーステーブルを追加。	修正済みソフトウェア	Final	2026年9月18日
1.0	初版リリース	—	Final	2026年9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の [シスコサポート & ダウンロード](#) 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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center \(TAC \)](#) 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。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。