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におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-asaftd-ikev2-dos-eBueGdEG
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCwo49925 CSCwq50506 CSCwo49926 CSCwq01516

CVE-2026-20015
CVE-2026-20013
CVE-2026-20014

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)ソフトウェアのインターネットキーエクスチェンジバージョン2(IKEv2)機能における複数の脆弱性により、リモート攻撃者がIKEv2パケットを解析する際にメモリをリークし、サービス妨害(DoS)状態を引き起こす可能性があります。

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-ikev2-dos-eBueGdEG

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、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確認

Cisco Secure Firewall ASAと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
```

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

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 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。

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-2026-20014:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのIKEv2 DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのIKEv2機能の脆弱性により、有効なVPNユーザクレデンシャルを持つ認証されたリモート攻撃者が、該当デバイスでDoS状態を引き起こし、ネットワーク内の他の場所にあるデバイスへのサービスの可用性にも影響を与える可能性があります。

この脆弱性は、IKEv2 パケットの不適切な処理に起因します。攻撃者は、巧妙に細工され、認証されたIKEv2パケット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。不正利用に成功すると、攻撃者はメモリを枯渇させ、デバイスのリロード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: CSCwq01516、CSCwq50506
CVE ID：CVE-2026-20014
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-2026-20013:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのIKEv2 DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのIKEv2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該当デバイスでDoS状態を引き起こし、ネットワーク内の他の場所にあるデバイスへのサービスの可用性に影響を与える可能性があります。

この脆弱性は、IKEv2パケット処理中にメモリを解放しないことによって引き起こされるメモリ枯渇に起因します。巧妙に細工された IKEv2 パケットを該当デバイスに送信することで、攻撃者が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、攻撃者はリソースを使い果たし、最終的にデバイスを手動でリロードする必要がある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: CSCwo49925
CVE ID：CVE-2026-20013

セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2026-20015:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのIKEv2 DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのIKEv2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該当デバイスでDoS状態を引き起こし、ネットワーク内の他の場所にあるデバイスへのサービスの可用性に影響を与える可能性があります。

この脆弱性は、IKEv2パケットを解析する際のメモリリークに起因します。巧妙に細工されたIKEv2 パケットを該当デバイスに送信することで、攻撃者が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、攻撃者はリソースを使い果たし、最終的にデバイスを手動でリロードする必要がある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: CSCwo49926
CVE ID：CVE-2026-20015
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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

これらの脆弱性は、Cisco Advanced Security Initiatives Group（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-ikev2-dos-eBueGdEG

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。