Cisco IOS、Cisco IOS XE、Cisco Secure Firewall 適応型セキュリティアプライアンス、Cisco Secure Firewall Threat Defense の各ソフトウェアの IKEv2 におけるサービス妨害（DoS）脆弱性

アドバイザリーID : cisco-sa-asa-ftd-ios-dos-DOESHWHy
初公開日 : 2025-08-14 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 : CSCwo15023 CSCwo15024 CSCwo49928 CSCwo15021 CSCwo15022 CSCwo49948 CSCwn83263 CSCwo15026 CSCwo20388 CSCwn73399

CVE-2025-20239
CVE-2025-20252
CVE-2025-20253
CVE-2025-20254
CVE-2025-20224
CVE-2025-20225

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 IOS ソフトウェア、Cisco IOS XE ソフトウェア、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、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、認証されていないリモートの攻撃者がサービス妨害（DoS）状態を引き起こす可能性があります。

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。これらの脆弱性には、回避策が存在します。

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。

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-asa-ftd-

ios-dos-DOESHWHy

このアドバイザリは、2025 年 8 月に公開された Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアのセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2025 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

CVE-2025-20225、CVE-2025-20239、CVE-2025-20253

この脆弱性は、IKEv2 VPN 機能が有効になっている次のシスコ製品に影響を与えます。

- IOS ソフトウェア
- IOS XE ソフトウェア
- Cisco Secure Firewall ASA ソフトウェア
- Cisco Secure FTD ソフトウェア

注：Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Group Encrypted Transport VPN（GET VPN）機能は影響を受けません。

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。

CVE-2025-20224、CVE-2025-20252、CVE-2025-20254

この脆弱性は、IKEv2 VPN 機能が有効になっている次のシスコ製品に影響を与えます。

- Cisco Secure Firewall ASA ソフトウェア
- Cisco Secure FTD ソフトウェア

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 IOS ソフトウェアおよび Cisco IOS XE ソフトウェアを実行している場合の IKEv2 設定の確認

Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行しているシスコデバイスの IKEv2 設定を判別するには、段階的な手順を使用してデバイスの動作ステータスと設定を正確に確認します。次の 2 段階の方法では、まずデバイスで IKEv1 または IKEv2 が有効になっているかどうか、次に IKEv2 がデバイスでアクティブに使用されているかどうかを判別します。

ステップ 1：IKE (v1 または v2) が有効になっているかどうかの確認

IKE 処理が有効になっているかどうかを確認するには、デバイスの CLI で show ip socket | include 500 または show udp | include 500 EXEC コマンドを使用します。UDP ポート 500 または UDP ポート 4500 がデバイスで開いている場合、そのデバイスは IKE パケットを処理しています。

注：IKEv1 または IKEv2 が有効になっている場合は、UDP ポート 500 または 4500 が開きます。これは、両方のプロトコルがこれらのポートを使用するためです。

UDP ポート 500 および 4500 で IPv4 または IPv6 のいずれかを使用して IKE パケットを処理しているデバイスの場合、show udp | include 500 コマンドの出力は次のようになります。

<#root>

```
Router#

show udp | include 500


 17       --listen--          192.168.1.10

500

   0   0 2001011   0
 17(v6)   --listen--          --any--

500

   0   0 2020011   0
 17       --listen--          192.168.1.10

4500

   0   0 2001011   0
 17(v6)   --listen--          --any--

4500

   0   0 2020011   0
```

このコマンドで空の出力が返される場合、デバイスはこれらの脆弱性の影響を受けません。統合されていない場合は、ステップ 2 に進んでください。

ステップ 2：IKEv2 が使用されているかどうかの確認

IKEv2 がデバイスでアクティブに使用されているかどうかを確認するには、デバイスの CLI で show crypto map EXEC コマンドを使用します。クリプトマップに IKEv2 プロファイル が関連付けられている場合、IKEv2 が使用されます。クリプトマップを使用しているインターフェイスが少なくとも 1 つある場合、そのクリプトマップはアクティブです。

IKEv2 パケットを処理しているデバイスの場合、show crypto map コマンドの出力は次のよう

になります。この出力では、クリプトマップ CMAP2 は IKEv2 プロファイル profile1 を使用するように設定され、インターフェイス GigabitEthernet2 で有効になっています。

```
<#root>

Router2#

show crypto map


Crypto Map IPv4 "

CMAP2

" 10 ipsec-isakmp
        Peer = 192.168.1.200


IKEv2 Profile: profile1


        Access-List SS dynamic: False
        Extended IP access list 120
            access-list 120 permit ip 192.168.21.0 0.0.0.255 192.168.22.0 0.0.0.255
        Current peer: 192.168.1.200
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Dualstack (Y/N): N

        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AESSET:  { esp-256-aes esp-sha256-hmac  } ,
        }
        Interfaces using crypto map

CMAP2

:


GigabitEthernet2


Router2#
```

このデバイスは、これらの脆弱性の影響を受けます。

Cisco Secure Firewall ASA および Cisco Secure FTD の各ソフトウェアを実行している場合の IKEv2 設定の確認

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。以下に、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 show running-config crypto ikev2 | include enable コマンド

の出力例を示します。

```
<#root>

firewall#

show running-config crypto ikev2 | include enable


crypto ikev2 enable

 outside client-services port 443
```

このデバイスは、これらの脆弱性の影響を受けます。 show running-config crypto ikev2 | include enable コマンドが空の出力を返す場合、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。

CVE-2025-20225、CVE-2025-20239、CVE-2025-20253

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- Cisco Secure Firewall Management Center（FMC）ソフトウェア

CVE-2025-20224、CVE-2025-20252、CVE-2025-20254

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XE ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- Cisco Secure FMC ソフトウェア

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-2025-20253：Cisco IOS、Cisco IOS XE、Cisco Secure Firewall ASA、Cisco Secure FTD の各ソフトウェアの IKEv2 における DoS 脆弱性

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco Secure Firewall ASA ソフトウェア、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。

この脆弱性は、IKEv2 パケットの不適切な処理に起因します。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。エクスプロイトが成功すると、攻撃者によってリソースを使い果たす無限ループが作成され、デバイスのリロード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：CSCwn73399、CSCwn83263
CVE ID：CVE-2025-20253
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-2025-20225、CVE-2025-20239：Cisco IOS、Cisco IOS XE、Cisco Secure Firewall ASA、Cisco Secure FTD の各ソフトウェアの IKEv2 における DoS 脆弱性

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco Secure Firewall ASA ソフトウェア、Cisco Secure FTD ソフトウェアの IKEv2 機能の 2 つの脆弱性により、認証されていないリモートの攻撃者がメモリリークを引き起こし、その結果 DoS 状態が発生する可能性があります。

これらの脆弱性は、IKEv2 パケットの不適切な処理に起因します。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、攻撃者がこれらの脆弱性をエクスプロイトする可能性があります。Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの場合、エクスプロイトが成功すると、攻撃者によって DoS 状態が引き起こされ、その結果、該当デバイスのリロードが発生する可能性があります。Cisco Secure Firewall ASA ソフトウェアおよび Cisco Secure FTD ソフトウェアの場合、エクスプロイトが成功すると、攻撃者によってシステムメモリが部分的に使い果たされ、新しい IKEv2 VPN セッションを確立できないといったシステムの不安定状態が発生する可能性があります。この状態から回復するには、デバイスを手動で再起動する必要があります。

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。

Cisco IOS および IOS XE ソフトウェア:

バグ ID：CSCwo20388
CVE ID：CVE-2025-20225

バグ ID：CSCwo49948
CVE ID：CVE-2025-20239

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

Cisco Secure Firewall ASA ソフトウェアおよび Cisco Secure FTD ソフトウェア：

バグ ID：CSCwo15022
CVE ID：CVE-2025-20225

バグ ID：CSCwo15023
CVE ID：CVE-2025-20239

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-2025-20224、CVE-2025-20252、CVE-2025-20254：Cisco Secure Firewall ASA ソフトウェアおよび Cisco Secure FTD ソフトウェアの IKEv2 における 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 機能の複数の脆弱性により、認証されていないリモートの攻撃者がメモリリークを引き起こし、その結果 DoS 状態が発生する可能性があります。

これらの脆弱性は、IKEv2 パケットの不適切な処理に起因します。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、攻撃者がこれらの脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者によってシステムメモリが部分的に使い果たされ、新しい IKEv2 VPN セッションを確立できないといったシステムの不安定状態が発生する可能性があります。この状態から回復するには、デバイスを手動で再起動する必要があります。

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。

バグ ID：CSCwo15026
CVE ID：CVE-2025-20224

バグ ID：CSCwo15024
CVE ID：CVE-2025-20252

バグ ID：CSCwo15021
CVE ID：CVE-2025-20254

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手でき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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS および IOS XE ソフトウェアの脆弱性による侵害の可能性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。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。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。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [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

Enter release number | Check

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-asa-ftd-ios-dos-DOESHWHy

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	2025 年 8 月 14 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。