Cisco Adaptive Security Appliance ソフトウェア、Firepower Threat Defense ソフトウェア、IOS ソフトウェア、および IOS XE ソフトウェアの IKEv2 におけるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-multiprod-ikev2-dos-gPctUqv2
初公開日 : 2025-05-07 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 : CSCwk40885 CSCwj99043

CVE-2025-20182

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 Adaptive Security Appliance（ASA）ソフトウェア、Cisco Firepower Threat Defense（FTD）ソフトウェア、Cisco IOS ソフトウェア、および Cisco IOS XE 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）プロトコル処理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が該当デバイスにサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、IKEv2 メッセージを処理する際の不十分な入力検証に起因します。攻撃者は、細工された IKEv2 トラフィックを該当デバイスに送信することによって、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、攻撃者がデバイスのリロードを引き起こし、該当デバイスで 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-multiprod-ikev2-dos-gPctUqv2

このアドバイザリは、2025 年 5 月に公開された Cisco IOS ソフトウェアおよび IOS XE ソフトウェアリリースのセキュリティ 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: May 2025 Semiannual Cisco IOS and IOS XE 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

この脆弱性は、Cisco ASA、FTD、IOS、または IOS XE ソフトウェアの脆弱性が存在するリリースを実行し、IKEv2 プロトコルが有効になっているシスコ製品に影響を与えます。

注：G-IKEv2 は、この脆弱性の影響を受けません。

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。

Cisco ASA または FTD ソフトウェアの IKEv2 設定の確認

インターフェイスで 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。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>

device#

show running-config crypto ikev2 | include enable


crypto ikev2 enable

outside
```

コマンドで出力が返されない場合、デバイスはこの脆弱性の影響を受けません。

注：Cisco FTD ソフトウェアを実行しているデバイスの場合、コマンドプロンプトは # ではなく > で終了します。

Cisco IOS または IOS XE ソフトウェアの IKEv2 設定の確認

1. デバイスに IKE (v1 または v2) が設定され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、CLI で show ip sockets または show udp EXEC コマンドを使用します。これらのコマンドでは、IKEv1 と IKEv2 の両方が同じポート番号を使用するため、両方とも同じ出力が表示されます。UDP ポート 500、UDP ポート

848、UDP ポート 4500、UDP ポート 4848 のいずれかがデバイスでオープンされている場合、そのデバイスは IKE パケットを処理しています。

以下に、UDP ポート 500 および UDP ポート 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での show udp コマンドの出力例を示します。

<#root>

```
router#
show udp

Proto      Remote      Port      Local        Port  In Out  Stat   TTY OutputIF
17       --listen--          192.168.130.21    500   0   0 1001011   0
17(v6)   --listen--          UNKNOWN           500   0   0 1020011   0
17       --listen--          192.168.130.21   4500   0   0 1001011   0
17(v6)   --listen--          UNKNOWN          4500   0   0 1020011   0
.
.
.
router#
```

コマンドで出力が返されない場合、またはコマンドでエラーが返される場合、デバイスはこの脆弱性の影響を受けません。デバイスから IKE の上記のいずれかの UDP ポートに関する出力が返される場合は、次の手順に進みます。

2. デバイスの IKE 設定が IKEv2 を使用しているかどうかの確認

show udp コマンドでデバイスが IKE トラフィックをリッスンしていることが示される場合、デバイスが IKEv2 を使用するように設定されているかどうかを調べるには、CLI コマンド show running-config | include ikev2 を入力します。コマンドの出力が返される場合、IKEv2 トラフィックを処理するように設定されている可能性が高いため、この脆弱性の影響を受けます。

注：一部のお客様は、適切な機能に関連付けずに IKEv2 コマンドを入力した可能性があります。完全な設定を確認したり、さまざまな show crypto ikev2 CLI コマンドの出力を調べたりすると、IKEv2 が正しく設定されているかどうかを確認するのに役立ちます。

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、この脆弱性が以下のシスコ製品には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（旧称 Firepower Management Center ソフトウェア）

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 ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性による問題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。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 ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 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 FTD デバイスのアップグレード手順については、該当の Cisco FMC アップグレードガイドを参照してください。

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

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

シスコは、この脆弱性を報告していただいたアメリカ国家安全保障局（NSA）に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multiprod-ikev2-dos-gPctUqv2

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 5 月 7 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。