Cisco IOS、IOS XE、Secure Firewall Adaptive Security Appliance、およびSecure Firewall Threat DefenseソフトウェアのIKEv2におけるDoS脆弱性

アドバイザリーID : cisco-sa-asa-ftd-ios-dos-kPEpQGGK
初公開日 : 2026-03-25 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 : CSCwq01523 CSCwq01495

CVE-2026-20012

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 Adaptive Security Appliance(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、該当デバイスでサービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、IKEv2パケットの不適切な解析に起因します。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。Cisco IOSソフトウェアおよびIOS XEソフトウェアの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。Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアの不正利用に成功すると、攻撃者がシステムメモリの一部を使い果たし、その結果、新しいIKEv2 VPNセッションを確立できないなど、システムが不安定になる可能性があります。この状態から回復するには、デバイスを手動でリブートする必要があります。

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-asa-ftd-

ios-dos-kPEpQGGK

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2026年3月リリースの一部です。これらのアドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 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、G-IKEv2を含む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

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ソフトウェアまたはIOS XEソフトウェアを実行しているデバイスでのIKEv2設定の確認

Cisco IOSソフトウェアまたはIOS XEソフトウェアを実行しているデバイスでIKEv1またはIKEv2が有効になっているかどうか、およびその後に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確認するには、次の2ステップの方法を使用します。

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

デバイスで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 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が有効な場合、どちらのプロトコルもこれらのポートを使用するため、UDPポート500、4500、またはその両方が開きます。

次の例は、UDPポート500および4500でIKEパケットを処理し、IPv4またはIPv6のいずれかをリスニングしているデバイスでのshow udp | include 500コマンドの出力を示しています。

<#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、デバイスはこの脆弱性の影響を受けません。コマンドの出力が返された場合は、ステップ2に進みます。

ステップ 2IKEv2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。少なくとも1つのインターフェイスがそのクリプトマップを使用している場合、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。出力では、暗号マップCMAP2は、IKEv2プロファイルprofile1を使用するように設定され、GigabitEthernet2インターフェイス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、この脆弱性の影響を受けます。

Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアを実行しているデバイスでのIKEv2設定の確認

Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアを実行しているデバイスで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。コマンドの出力が返された場合は、少なくとも1つのインターフェイスでIKEv2が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、この脆弱性の影響を受けます。

show running-config crypto ikev2 | include enableコマンドで空の出力が返される場合、そのデバイスは、こ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
- NX-OS ソフトウェア
- Cisco Secure Firewall Management Center（FMC）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 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

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）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 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-kPEpQGGK

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25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。