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1におけるサービス妨害(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-iosxe-ikev1-dos-XHk3HzFC
初公開日 : 2025-05-07 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 : CSCwi26594

CVE-2025-20192

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 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1(IKEv1)実装における脆弱性により、認証されたリモート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。攻撃者がこの脆弱性を不正利用するには、有効なIKEv1 VPNクレデンシャルが必要です。

この脆弱性は、IPsecセキュリティアソシエーション(SA)作成要求が該当デバイスのハードウェア暗号化アクセラレータに渡される前の、IKEv1フェーズ2パラメータの検証が不適切なことに起因します。攻撃者は、巧妙に細工されたIKEv1メッセージ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。エクスプロイトに成功すると、攻撃者は標的デバイスのリロードを引き起こすことができるようになります。

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-iosxe-ikev1-dos-XHk3HzFC

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ソフトウェアのセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』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 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、IKEv1 VPNが有効になっている次のシスコ製品に影響を与えます。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ ISR
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Catalyst 8500 シリーズ エッジ プラットフォーム
- Catalyst 8500L シリーズ エッジ プラットフォーム

次の機能は、IKEv1を使用するように設定されている場合、この脆弱性の影響を受けます。

- Dynamic Multipoint VPN（DMVPN）
- リモートアクセスIPsec VPN(RAVPN)
- サイト間VPN(S2S VPN)

注：Cisco Group Encrypted Transport VPN(GET VPN)およびSSL VPNは、IPsecセッションの確立にIKEv1を使用しないため、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。

デバイス設定の確認

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：UDPポート500または4500、あるいはその両方は、IKEv1とIKEv2のどちらが有効になっているかに関係なく、両方とも同じポート番号とプロトコル番号を使用するため、オープンになります。

次の例は、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た場合、デバイスはこ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。

2. IKEv1が使用されているかどうかの判別

IKEv1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。IKEv2プロファイルが関連付けられていない場合、クリプトマップではIKEv1が使用されます。暗号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、その暗号マップはアクティブです。

次に、IKEv1を使用するように設定され(IKEv2 Profileがリストされていないため)、インターフェイスGigabitEthernet1で有効化されている暗号マップCMAP1があるデバイスでのshow crypto mapコマンドの出力例を示します。

<#root>

```
Router1#

show crypto map


Crypto Map IPv4 "CMAP1" 10 ipsec-isakmp
        Peer = 192.168.1.100
        Access-List SS dynamic: False
        Extended IP access list 120
            access-list 110 permit ip 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255
        Current peer: 192.168.1.100
        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

 CMAP1:
                GigabitEthernet1


Router1#
```

このデバイスは、この脆弱性の影響を受けます。

次に、IKEv2を使用するように設定され(IKEv2 Profileがリストされているため)、インターフェイスGigabitEthernet2で有効化されている暗号マップCMAP2があるデバイスでのshow crypto mapコマンドの出力の例を示します。

<#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#
```

デバイスに設定されている暗号マップがこの暗号マップだけである場合、こ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 ソフトウェア
- 「脆弱性が存在する製品」セクションに記載されているデバイス以外のデバイスで実行されている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

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 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

この脆弱性は Cisco 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-iosxe-ikev1-dos-XHk3HzFC

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

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。