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 Software for Firepower 2100シリーズのIPv6 over IPsecにおけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-fp2k-IPsec-dos-tjwgdZCO
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 : CSCwm95070

CVE-2025-20222

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 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IPsec VPN機能のRADIUSプロキシ機能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、IPv6パケットの不適切な処理に起因します。攻撃者は、IPsec VPN接続経由で該当デバイスにIPv6パケットを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。

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-fp2k-IPsec-dos-tjwgdZCO

このアドバイザリは、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2025年8月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: 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

この脆弱性は、Cisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアの脆弱性が存在するリリースを実行し、かつ次の条件をすべて満たしているCisco Firepower 2100シリーズファイアウォールに影響を与えます。

- インターネットキーエクスチェンジバージョン1(IKEv1)またはIKEv2を使用するIPsec VPNが有効になっている。
- RADIUSトラフィックを受信しているインターフェイスでIPv6が有効になっている。
- アクセスコントロールリスト(ACL)は、IPトラフィックを許可するように設定されます。

IKEv1 VPN設定の確認

IKEv1 VPNはどのインターフェイスでもデフォルトで有効になっていません。

いずれかのインターフェイスでIKEv1 VPNが有効になっているかどうかを確認するには、show running-config crypto ikev1 | include crypto ikev1 enable CLIコマンドを使用します。このコマンドの出力が空でない場合は、リストされている1つまたは複数のインターフェイスでIKEv1 VPNが有効になっていることを示します。空の出力は、IKEv1 VPNがどのインターフェイスでも有効になっていないことを示します。

次に、外部インターフェイスでIKEv1 VPNが有効になっているデバイスでのshow running-config crypto ikev1 | include crypto ikev1 enableコマンドの出力例を示します。

```
<#root>

> show running-config crypto ikev1 | include crypto ikev1 enable

crypto ikev1 enable outside
```

IKEv2 VPN設定の確認

IKEv2 VPNはどのインターフェイスでもデフォルトで有効になっていません。

いずれかのインターフェイスでIKEv2 VPN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 crypto ikev2 enable CLIコマンドを使用します。このコマンドの出力が空でない場合は、リストされたインターフェイスでIKEv2 VPNが有効になっていることを示します。空の出力は、IKEv2 VPNがどのインターフェイスでも有効になっていないことを示します。

次に、外部インターフェイスでIKEv2 VPNが有効になっているデバイスでのshow running-config crypto ikev2 | include crypto ikev2 enableコマンドの出力例を示します。

```
<#root>

> show running-config crypto ikev2 | include crypto ikev2 enable

crypto ikev2 enable outside
```

注：crypto ikev2 enableコマンドでは、オプションのportパラメータを含むことのできる追加のclient-servicesオプションを指定できます。これらのオプションは、デバイスがこの脆弱性の影響を受けるかどうかには影響しません。

IPv6設定の確認

IPv6が有効になっているデバイスで、IPv6アドレスが割り当てられているインターフェイスを確認するには、次の例に示すようにshow running-config | include interface | ipv6 CLIコマンドを使用します。

```
<#root>

>

show running-config interface | include interface | ipv6

interface GigabitEthernet0/0

 ipv6 address

 2001:db8:0:1:192:168:1:12/64

 ipv6 enable
```

ACL設定の決定

コントロールプレーンACLが設定されているかどうかを確認するには、show running-config access-group | include control-planeコマンドを使用します。コントロールプレーンACLが設定されていない場合、デバイスはこの脆弱性の影響を受けません。

上記のコマンドの出力に含まれるACLのACL-list-nameを使用して、show access-list ACL-list-nameを実行し、ACLがIPトラフィックを許可するように設定されているかどうかを確認します。最初のコマンドの出力に複数のACLが表示される場合は、各ACLを確認します。

次に、ACL ACL-list-nameがIPトラフィックを許可するように設定されているデバイスでのコマンドの出力例を示します。

```
<#root>

>

show running-config access-group | include control-plane


 access-group

ACL-list-name

 in interface outside control-plane

> show access-list

ACL-list-name


  access-list

ACL-list-name

 line 1 extended permit ip any6 any6
```

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。

- 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プラットフォーム以外のプラットフォームで実行している場合は、ファイアウォールASAソフトウェアを保護してください
- 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プラットフォーム以外のプラットフォームで実行している場合は、FTDソフトウェアを保護してください
- 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 Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェア

お客様がCisco Secure Firewall ASA、Secure FMC、およびSecure FTD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。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9.16.2.11、Cisco Secure 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 Secure FTDデバイスのアップグレード手順については、該当する『Cisco Secure FMC upgrade guide』を参照してください。

関連情報

最適なCisco Secure Firewall ASA、Secure FMC、またはSecure FTDソフトウェアリリースの判別に関しては、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 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-fp2k-IPsec-dos-tjwgdZCO

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。