# Cisco Secure Firewall Management CenterソフトウェアのRADIUSにおけるリモートコード実行の脆弱性


アドバイザリーID : cisco-sa-fmc-radius-rce-TNBKf79
CVE-2025-20265
初公開日 : 2025-08-14 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwo91250

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 Management Center(FMC)ソフトウェアのRADIUSサブシステム実装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、デバイスで実行される任意のシェルコマンドを挿入する可能性があります。

この脆弱性は、認証フェーズでユーザ入力が適切に処理されないことに起因します。攻撃者は、設定されたRADIUSサーバで認証されるクレデンシャルを入力する際に、巧妙に細工された入力を送信することで、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、攻撃者は高い特権レベルでコマンドを実行できる可能性があります。

注：この脆弱性をエクスプロイトするには、Webベースの管理インターフェイスのRADIUS認証、SSH管理、またはその両方で、Cisco Secure FMCソフトウェアを設定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-fmc-radius-rce-TNBKf79

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

Cisco Secure FMCソフトウェアリリース7.0.7および7.7.0でRADIUS認証が有効になっている場合にのみ、この脆弱性の影響を受けます。RADIUSが設定されているかどうかを確認する方法の手順については、『Cisco Secure Firewall Management Centerアドミニストレーションガイド』の「Management Center用のRADIUS外部認証オブジェクトの追加」を参照してください。

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。

### 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Cisco Secure Firewall Adaptive Security Appliance(ASA)ソフトウェアまたはCisco Secure Firewall Threat Defense(FTD)ソフトウェアには影響を与えないことを確認しました。

## 回避策

この脆弱性に対処する回避策はありません。

ただし、この脆弱性を不正利用できるのは、Cisco Secure FMCソフトウェアでRADIUS認証が設定されている場合だけです。この脆弱性を軽減するには、ローカルユーザアカウント、外部LDAP認証、SAMLシングルサインオン(SSO)など、別のタイプの認証を使用します。 詳細については、『Cisco Secure Firewall Management Center Administration Guide』を参照してください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 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。

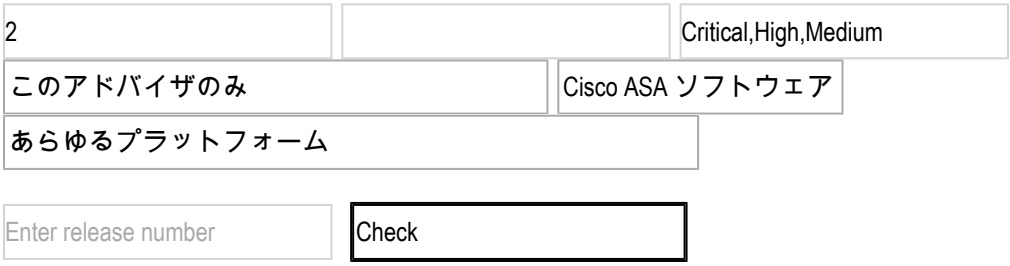
## Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェア

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。




### 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、シスコ内部でセキュリティテストを実施中、シスコの Brandon Sakai によって発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79

## 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。