

Cisco Secure Firewall適応型セキュリティアプライアンス、Secure Firewall Threat Defense、およびSecure Firewall Management Centerソフトウェアの強化リリース：2026年9月



Advisory ID : cisco-sa-hardening-asaftdfmc-[CVE-2026-20329](#)
uvpPROhN
初公開日 : 2026-09-16 16:00 [CVE-2026-20336](#)
最終更新日 : 2026-09-18 15:50 [CVE-2026-20334](#)
バージョン 1.1 : Final [CVE-2026-20335](#)
CVSSスコア : [9.9](#) [CVE-2026-20332](#)
回避策 : No workarounds available [CVE-2026-20333](#)
Cisco Bug ID : [CVE-2026-20330](#)
[CVE-2026-20331](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco Secure Firewall Adaptive Security Appliance(ASA)ソフトウェア、Cisco Secure Firewall Threat Defense(FTD)ソフトウェア、およびCisco Secure Firewall Management Center(FMC)ソフトウェアエンジニアリングチームは、包括的な内部セキュリティレビューを実施しました。このレビューの結果、社内で発見された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は、シスコの社内テストで発見されたものです。そのうち2つは活発に不正利用されていることが確認されています。詳細については、次のアドバイザリを参照してください。

[Cisco Secure Firewall Management Centerソフトウェアの静的クレデンシャルの脆弱性](#)および
[Cisco Secure Firewall Management Centerソフトウェア認証バイパスの脆弱性](#)お客様によるパッ

チ適用を支援し、開示プロセスを効率化するために、シスコはこれらの問題をその根本的な脆弱性クラス (Common Weakness Enumeration (CWE)) ごとに分類し、CWE の各グループに 1 つの共通脆弱性識別子 (CVE ID) を割り当てました。

シスコはこれら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。これら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-hardening-asaftdfmc-uvpPROhN>

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、[2026年9月16日発行のCisco Advance Notification, Security Advisories](#)を参照してください。

該当製品

脆弱性がある製品

これらの脆弱性は、デバイスの設定に関係なく、次のシスコ製品に影響を与えます。

- Cisco Secure Firewall ASA ソフトウェア
- Cisco Secure FTD ソフトウェア
- Cisco Secure FMC 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。

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](#)」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

次の表に、この強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ (重大度) を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルの CWE)	説明
CVE-2026-20329	9.9	CWE-703	例外条件の不適切な処理 (不明な例外、到達可能なアサーションを含む)

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルのCWE)	説明
CVE-2026-20330	9.9	CWE-707	構造化されたメッセージまたはデータが整形形式であり、アップストリームコンポーネントから読み取られる前、またはダウンストリームコンポーネントに送信される前に特定のセキュリティプロパティが満たされることが誤って保証される
CVE-2026-20331	9.6	CWE-693	製品に対する標的型攻撃に対して十分な防御を提供する保護メカニズムを誤って使用している
CVE-2026-20332	9.0	CWE-284	不適切なアクセスコントロール (許可、認証、特権、バイパスを含む) ¹
CVE-2026-20333	8.8	CWE-697	セキュリティ関連のコンテキストにおける2つのエンティティの比較が正しくない
CVE-2026-20334	8.4	CWE-710	コーディング標準への不適切な準拠
CVE-2026-20335	8.1	CWE-682	誤った結果や意図しない結果を生成し、後でセキュリティ・クリティカルな決定やリソース管理に使用する計算
CVE-2026-20336	7.5	CWE-664	ライフタイム期間中のリソースの不適切な制御 (初期化されていない変数、NULL ポインタ、リソースのライフサイクルの問題など)

1. この脆弱性クラスに属する2つの脆弱性が、活発に不正利用されることが確認されています。詳細については、『[Cisco Secure Firewall Management Centerソフトウェアスタティックレディンシャルの脆弱性](#)』および『[Cisco Secure Firewall Management Centerソフトウェア認証バイパスの脆弱性](#)』を参照してください。

回避策

これら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

これらの脆弱性を修正し、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。

修正リリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。中央の列には、このアドバイザリで説明されている脆弱性の影響を受けるホットフィックスを、右側の列にはこれらの脆弱性に対する修正が含まれる最初のソフトウェアリリースを示します。上記のホットフィックスリリースのいずれかをインストールしたお客様は、上記の最初の修正リリースをインストールする必要があります。

Cisco Secure Firewall ASA ソフトウェアリリース	該当するホットフィックスリリース	第 1 修正済みリリース
9.16 以前	N/A	9.16.4.103
9.18	9.18.4.135	9.18.4.94
9.20	9.20.4.235	9.20.4.49
9.22	9.22.3.191	9.22.3.26
9.23	9.23.1.195 9.23.1.211	9.23.1.47
9.24	9.24.1.155 9.24.1.221	9.24.1.26

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。

Cisco Secure FTDソフトウェアリリースおよびSecure FMCソフトウェアリリース	第 1 修正済みリリース
7.0 以前	7.0.10
7.2	7.2.12
7.4	7.4.8
7.6	7.6.6
7.7	7.7.13
10.0	10.0.2
10.1	10.1.0

複数の脆弱性に対する修正が含まれているため、上記の表の最初の修正済みリリースにアップグレードすることを強くお勧めします。詳細は、『[Cisco Secure Firewall適応型セキュリティアプライアンス、Secure Firewall Threat Defense、およびSecure Firewall Management Centerソフトウェアの強化リリース：2026年9月](#)』を参照してください。

シスコの Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

すでに特記されている場合を除き、Cisco PSIRTでは、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とその公表は確認しておりません。

出典

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した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-hardening-asaftdfmc-uvpPROhN>

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	ASA修正済みリリースの表を更新。	修正リリース	Final	2026年9月18日
1.0	初版リリース	—	Final	2026年9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center \(TAC \)](#) 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。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の [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アップグレード ソリューション一式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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。