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ソフトウェアのオブジェクトグループアクセスコントロールリストのバイパスの脆弱性

Advisory ID : cisco-sa-ftd-acl-bypass-8p6vFvw
初公開日 : 2026-09-16 16:00
最終更新日 : 2026-09-18 15:50
バージョン 1.1 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco Bug ID : CSCwr49050 CSCwr04957

CVE-2026-20121
CVE-2026-20120

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

Cisco Secure Firewall適応型セキュリティアプライアンス(ASA)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアのアクセスコントロールリスト(ACL)オブジェクトグループ検索(OGS)実装における複数の脆弱性により、認証されていないリモートの攻撃者が、設定されたアクセスコントロールをバイパスできる可能性があります。

これらの脆弱性は、OGSが設定されたグループアクセスコントロールポリシー(ACP)に論理エラーが設定されていることに起因します。攻撃者は、デバイスを介してブロックする必要のあるトラフィックを送信することで、これら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、攻撃者はアクセスコントロールをバイパスし、保護されたネットワーク内のデバイスに到達できる可能性があります。

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-ftd-acl-bypass-8p6vFvw

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。また、Cisco Secure Firewall製品の改善と修正に関するさらに詳しいドキュメントについては、『Cisco Secure Firewall Adaptive Security Appliance Software、Secure Firewall Threat Defense Software、およびSecure Firewall Management Centerソフトウェア強化リリース：2026年9月』を参照してください。

該当製品

脆弱性がある製品

公開時点では、シスコデバイスでCisco Secure Firewall ASAソフトウェアまたはCisco Secure FTDソフトウェアの脆弱性が存在するリリースが実行されており、OGSが設定されたACLが存在する場合、これらの脆弱性の影響を受けます。

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 Secure FTDソフトウェアを実行しているデバイスでのACL OGS設定の確認

Cisco Secure FTDソフトウェアを実行しているデバイスで、OGSを使用するACLが設定されているかどうかを確認するには、Cisco Secure Firewall Management Center(FMC)ソフトウェアで次の手順を実行します。

1. Objects > Object Managementの順に選択します。
2. オブジェクトタイプを選択します（例：Network）。
3. 一覧表示されているオブジェクトグループを表示します。

オブジェクトグループがリストされていない場合、デバイスはこれらの脆弱性の影響を受けません。

Cisco Secure Firewall ASAソフトウェアを実行しているデバイスでのACL OGS設定の確認

デバイスでCisco Secure Firewall ASAソフトウェアが実行されており、ACP用にOGSを使用して設定されているかどうかを確認するには、次の例で示すように、CLIコマンドshow running-config object-group-searchを使用します。

```
<#root>

ciscoasa#

show running-config object-group-search


object-group-search access-control
```

出力でオブジェクトグループのリストが返されない場合、デバイスはこれら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。

シスコは、これらの脆弱性が Cisco Secure FMC ソフトウェアには影響を与えないことを確認しました。

詳細

これらの脆弱性がエクスプロイトされると、攻撃者は該当デバイスに適用されるACLによって提供される保護をバイパスできる可能性があります。この脆弱性の悪用による影響はACLで保護されるはずの資産の重要性に依存しているため、全体として組織に固有です。お客様は、これらの脆弱性の不正利用がお客様のネットワークに与える影響を評価し、お客様自身の脆弱性処理および修復プロセスに従って処理を進める必要があります。

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

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
9.20 以前	N/A	脆弱性なし
9.22	9.22.3.191	9.22.3.26
9.23	9.23.1.195	9.23.1.47

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
	9.23.1.211	
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
7.4 以前	脆弱性なし
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。

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	

Cisco Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC アップグレードガイドを参照してください。

その他のリソース

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新しいリリースが推奨される場合、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）では、本アドバイザリに記載されている脆弱性のエクスプロイト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、Cisco Technical Assistance Center(TAC)の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-ftd-acl-bypass-8p6vFvw

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	修正済みリリーステーブルを追加します。	修正済みソフトウェア	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。