Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower脅威対策ソフトウェアのAnyConnectアクセスコントロールリストのバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-ac-acl-bypass-bwd7q6Gb
初公開日 : 2023-11-01 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwe45093 CSCwd30856

CVE-2023-20245
CVE-2023-20256

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CiscoFirepower脅威対策(FTD)ソフトウェアのユーザごとの上書き機能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リスト(ACL)をバイパスし、拒否すべきトラフィックが該当デバイスを通過できるようになる可能性があります。

これらの脆弱性は、影響を受けるソフトウェアがユーザごとの上書きルールを作成して適用するときに発生する可能性がある論理エラーに起因します。攻撃者は、脆弱性のある設定を持つ該当デバイスを介してネットワークに接続することで、これらの脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はインターフェイスACLをバイパスし、保護する必要があるリソースにアクセス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-asaftd-ac-acl-bypass-bwd7q6Gb

このアドバイザリは、Cisco ASA、FTD、およびFMCセキュリティアドバイザリバンドル公開の2023年11月版リリースの一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: November 2023 Semiannual Cisco ASA, FMC, and 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

公開時点で、これらの脆弱性は、Cisco ASAまたはFTDソフトウェアの脆弱性が存在するリリースを実行し、次の条件をすべて満たすシスコ製品に影響を与えました。

- sysopt connection permit-vpnコマンド（VPNトンネルを介してセキュリティアプライアンスに入るトラフィックがインターフェイスACLをバイパスできるようにする）がディセーブルにされていました。
- 少なくとも1つのインターフェイスACLでユーザごとのオーバーライド機能(ユーザごとのオーバーライド)が有効になっています。
- 少なくとも1つのリモートアクセスVPN接続プロファイル(tunnel-group)またはサイト間VPN接続プロファイル(tunnel-group)が設定されていて、フィルタACL(vpn-filter)を指定するグループポリシー(group-policy)に関連付けられていました。
- 影響を受ける接続プロファイル(tunnel-group)に関連付けられたVPNトンネルが現在稼働していました。

注：Cisco FTDソフトウェアでは、FlexConfigでのみユーザごとのオーバーライド機能を有効にできます。

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。

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。

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

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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスク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、セキュリティ影響評価（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 ASA ソフトウェアの場合は 9.16.2.11、Cisco 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	

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

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 TAC のサポート案件の対応時に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ac-acl-bypass-bwd7q6Gb

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	2023年11月1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。