Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアの AnyConnectアクセスコントロールリストバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-acl-bypass-VvnLNKqf
初公開日 : 2024-10-23 16:00
最終更新日 : 2024-10-24 21:19
バージョン 1.1 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwd96845 CSCwf23262

CVE-2024-20297
CVE-2024-20299

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Cisco Firepower Threat Defense(FTD)ソフトウェアのAnyConnectファイアウォール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、拒否されるはずの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、AnyConnectクライアントが影響を受けるデバイスに対して新しいセッションを確立するときに、グループACLに論理エラーを設定することに起因します。攻撃者は、該当デバイスへのAnyConnect接続を確立することで、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、攻撃者は設定されたACLルールをバイパ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-acl-bypass-VvnLNKqf

このアドバイザリは、2024年10月に公開されたCisco ASA、FMC、およびFTDソフトウェアセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、

『シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月』を参照してください。

該当製品

脆弱性のある製品

公開時点では、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ていて、前方参照とAnyConnectファイアウォールルール機能が有効になっているシスコデバイスに影響を与えました。

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。

デバイス設定の確認

前方参照およびAnyConnectファイアウォールルール機能がデバイスで有効になっているかどうかを確認するには、show running-config CLIコマンドを使用します。

Cisco ASAソフトウェアリリース9.18.1またはCisco FTDソフトウェアリリース7.2.0より前のリリースを実行しているデバイスの場合は、forward-reference enable とanyconnect firewall-rule client-interfaceの出力を調べます。両方のコマンドが存在する場合、デバイスはこれらの脆弱性の影響を受けます。

Cisco ASAソフトウェアリリース9.18.1以降またはCisco FTDソフトウェアリリース7.2.0以降を実行しているデバイスの場合、前方参照はデフォルトで有効になっており、無効にすることはできません。anyconnect firewall-rule client-interfaceのshow running-config CLIコマンドの出力を調べます。コマンドが存在する場合は、オブジェクトグループが宛先ネットワークまたは宛先ポート、あるいはその両方としてコマンドに設定されているかどうかを判別します。

- オブジェクトグループを宛先ネットワークとして使用すると、結果としてクライアントにプッシュされるACLのみに、任意の宛先ネットワーク(0.0.0.0/0)への許可ルールが含まれます。
- オブジェクトグループを宛先ポートとして使用すると、結果としてクライアントにプッシュされるACLのみに、任意の宛先ポート(1 ~ 65535)への許可ルールが含まれます。
- オブジェクトグループを宛先ネットワークと宛先ポートの両方として使用した場合、結果としてクライアントにプッシュされるACLには、任意の宛先ポート(1 ~ 65535)上の任意の宛先ネットワーク(0.0.0.0/0)に対する許可ルールが含まれます。

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 Firewall Management Center(FMC)ソフトウェア（旧Firepower Management Center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

注：Cisco ASAソフトウェアを実行しているCisco 3000シリーズ産業用セキュリティアプライアンス(ISA)については、Cisco ASAソフトウェアリリース9.16.4.67のリリースは延期されており、リリース9.16.4.70に置き換えられています。

Cisco 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 FMC upgrade guide』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-acl-bypass-VvnLNKqf

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	CLIコマンドでハイフンを削除。	脆弱性が存在する製品	Final	2024年10月24日
1.0	初回公開リリース	—	Final	2024年10月23日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンド

ユーザを対象としています。

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。