Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアの非アクティブからアクティブへのACLバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-ogsnsg-aclbyp-3XB8q6jX
CVE-2024-20293
初公開日 : 2024-05-22 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwi17713

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)ソフトウェアのアクセスコントロールリスト(ACL)のアクティベーション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、該当デバイスに設定されたACLによる保護をバイパスできる可能性があります。

この脆弱性は、該当デバイスの実行コンフィギュレーションでACLが非アクティブからアクティブに変更されたときに発生する論理エラーに起因します。攻撃者は、設定されたACLによって拒否されるべき該当デバイスを介してトラフィックを送信することにより、この脆弱性を不正利用する可能性があります。逆の条件も成立します。許可すべきトラフィックが、設定されたACLによって拒否される可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスで設定されているACL保護をバイパスし、デバイスが保護している信頼できるネットワークにアクセスできる可能性があります。

注：この脆弱性は、IPv4とIPv6の両方のトラフィック、およびIPv4とIPv6の両方のACLがインターフェイスに設定されているデュアルスタックACL設定に適用されます。

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-asaftd-

ogsnsg-aclbyp-3XB8q6jX

このアドバイザリは、2024年5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5月』を参照してください。

該当製品

脆弱性のある製品

この脆弱性の公開時点では、脆弱性のある設定で次のいずれかのシスコソフトウェアリリースを実行しているシスコ製品が、この脆弱性の影響を受けています。

- ASAソフトウェアリリース9.19.1 ~ 9.19.1.24、9.20.1、または9.20.1.5
- FTDソフトウェアリリース7.3.0 ~ 7.4.0

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。

デバイスの設定に脆弱性があるかどうかの確認

このACLバイパスの脆弱性は、特定の設定が原因で発生するもので、アクセスリストを非アクティブからアクティブに変更する必要があります。脆弱性のある設定は、次の条件を満たす必要があります。

- この箇条書きリストに続くrunning-configのobject-group-search access-controlコマンドによって示されるように、オブジェクトグループ検索(OGS)のACL最適化機能が有効になっています。
- 非アクティブとして設定されたアクセスリストには、オブジェクトグループネットワークサービス(NSG)[1]がありませんが、ネットワークオブジェクトグループは含まれています。次の例では、ネットワークオブジェクトグループはsample1です。

上記の2つの条件が満たされて、アクセスリストがinactiveからactiveに変更された場合、変更は有効にならず、ユーザに対する警告も表示されません。次の例では、アクセスリストはCSM_FW_ACL_です。

この設定の一部を示す次の例では、アクセスリストCSM_FW_ACL_がアクティブにならず、その結果トラフィックがそのルールに一致しなくなります。

```
<#root>

device#

show running-config
```

```
.
.
.
object-group-search access-control
.
.
.
object-group network sample1
 network-object host 192.168.1.2
.
.
.
access-group CSM_FW_ACL_ global
.
.
.
access-list
CSM_FW_ACL_
 extended permit ip host 192.168.1.1 object-group sample1
inactive


access-group CSM_FW_ACL_ global
.
.
.
```

1. NSG設定については、『Cisco Secure Firewall ASAシリーズコマンドリファレンス、I - Rコマンド：object network-service』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、この脆弱性が Cisco Firepower Management Center（FMC）ソフトウェアに影響を及ぼさ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。動作していないアクセスリストを削除して、この脆弱性を回避できるように再設定できます。このアドバイザリの「脆弱性が存在する製品」セクションの設定例を使用して、次のCLIコマンドを実行します。

```
device# no access-list CSM_FW_ACL_ extended permit ip host 192.168.1.1 object-group sample1
device# access-list CSM_FW_ACL_ extended permit ip host 192.168.1.1 object-group sample1
```

この回避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

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 | オン

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

関連情報

最適な Cisco ASA、FMC、または FTD 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 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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ogsnsg-aclbyp-3XB8q6jX

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	2024年5月22日

利用規約

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。