Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアにおける認証バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-saml-bypass-KkNvXyKW
CVE-2024-20355
初公開日 : 2024-05-22 16:00
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No workarounds available
Cisco バグ ID : CSCwe95729

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)ソフトウェアのリモートアクセスVPNサービス向けのSAML 2.0シングルサインオン(SSO)の実装における脆弱性により、認証されたリモートの攻撃者が、該当デバイスでVPNセッションを正常に確立できる可能性があります。

この脆弱性は、SAML認証を使用する際の認証ドメインの不適切な分離に起因します。攻撃者は、有効なクレデンシャルを使用して指定された接続プロファイル（トンネルグループ）で正常に認証を行い、Cisco ASAデバイスから返信されたSAML SSOトークンを傍受し、同じSAML SSOトークンを別のトンネルグループに送信して認証を受けることで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者は使用が許可されていない接続プロファイルを使用してリモートアクセスVPNセッションを確立し、アクセスが許可されていない該当デバイスの背後にあるセキュアなネットワークに接続できる危険性があります。不正利用に成功するには、攻撃者は有効なリモートアクセスVPNユーザクレデンシャルを持っている必要があります。

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-saml-bypass-KkNvXyKW

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、Cisco ASAソフトウェアまたはFTDソフトウェアを実行していて、SAML 2.0 SSOでリモートアクセスVPNを設定しているシスコ製品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。

リモートアクセスVPN SAML認証設定の決定

認証にSAML 2.0を使用するように設定されているリモートアクセスVPN接続プロファイル（トンネルグループ）の数を確認するには、show running-config tunnel-group | count authentication.*saml CLIコマンドを使用します。コマンドの出力に、2以上の数の一致行が表示された場合、そのデバイスはこの脆弱性の影響を受けます。次の例は、show running-config tunnel-group | count authentication.*samlコマンドを、SAML 2.0 SSO認証を使用するように設定された2つの接続プロファイル（トンネルグループ）を持つデバイスで実行した場合の処理を示します。

```
<#root>

device#

show running-config tunnel-group | count authentication.*saml


Number of lines which match regexp =

2
```

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。

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

この脆弱性は Cisco TAC 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-asaftd-saml-bypass-KkNvXyKW

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。