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Firepowerの脅威対策ソフトウェアのリモートアクセスSSL VPNにおける複数の証明書認証バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-multi-cert-dzA3h5PT
CVE-2023-20247
初公開日 : 2023-11-01 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 : CSCwe20918

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)ソフトウェアのリモートアクセスSSL VPN機能の脆弱性により、認証されたリモートの攻撃者が、設定された複数の証明書認証ポリシーをバイパスし、有効なユーザ名とパスワードのみを使用して接続する可能性があります。

この脆弱性は、リモートアクセスVPN認証時の不適切なエラー処理に起因します。攻撃者は、リモートアクセスVPNセッションの確立中に巧妙に細工された要求を送信することで、こ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、元の接続プロファイルに関連付けられた特権と権限を維持したまま、設定された複数の証明書認証ポリシーをバイパスできる可能性があります。

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-multi-cert-dzA3h5PT

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

公開時点では、この脆弱性は、Cisco ASAソフトウェアまたはFTDソフトウェアの脆弱性が存在するリリースを実行し、複数の証明書認証を必要とする少なくとも1つの設定プロファイルでリモートアクセスSSL VPN機能を有効にし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。

リモートアクセスSSL VPN設定の確認

リモートアクセスVPNの設定を確認するには、show running-config webvpn | include ^ enable CLIコマンドを使用します。コマンドの出力が返された場合は、表示されているインターフェイスでリモートアクセスSSL VPN機能が有効になっています。出力が空の場合は、リモートアクセスSSL VPN機能が有効になっていないことを示しています。次に、show running-config webvpn | include ^ enableコマンドを、outsideインターフェイスでリモートアクセスSSL VPN機能が有効になっているデバイスで実行した場合の出力例を示します。

```
<#root>

asa#

show running-config webvpn | include ^ enable


enable

 outside
```

リモートアクセスSSL VPN機能が少なくとも1つのインターフェイスで有効になっている場合は、show running-config tunnel-group | include multiple-certificate CLIコマンドを使用して、複数の証明書認証を必要とする接続プロファイルが設定されているかどうかを評価します。コマンドの出力が返された場合は、複数の証明書認証を必要とする設定プロファイルが少なくとも1つ設定されています。空の出力は、デバイスで複数の証明書認証が使用されていないことを示します。次の例は、show running-config tunnel-group | include multiple-certificateコマンドを、複数の証明書認証を必要とする1つの設定プロファイルが設定されているデバイスで実行した場合の出力例を示します。

```
<#root>
```

```
asa#
show running-config tunnel-group | include multiple-certificate


authentication multiple-certificate
```

上記のコマンドの一方または両方が空の出力を返す場合、デバイスはこ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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Firepower Management Center（FMC）ソフトウェア
- IOS ソフトウェア
- IOS XE ソフトウェア
- IOS XR ソフトウェア
- 次世代侵入防御システム（NGIPS）ソフトウェア
- NX-OS ソフトウェア

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。

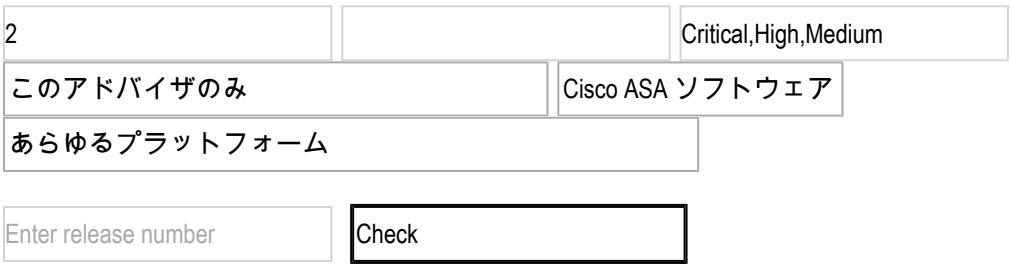
Cisco ASA、FMC、および FTD ソフトウェア

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。



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。

関連情報

最適な Cisco ASA、FTD、または FMC 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

シスコは、この脆弱性を報告していただいたDeutsche Telekom MMS GmbH社のTobias Moritz氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-multi-cert-dzA3h5PT

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。