

Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアのダイナミックアクセスポリシーにおけるサービス妨害の脆弱性



アドバイザリーID : cisco-sa-asaftd-dap-dos-bhEkP7n

[CVE-2024-20408](#)

初公開日 : 2024-10-23 16:00

バージョン 1.0 : Final

CVSSスコア : [7.7](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwj15792](#)

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)ソフトウェアのダイナミックアクセスポリシー(DAP)機能の脆弱性により、認証されたリモートの攻撃者が該当デバイスの予期しないリロードを引き起こす可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスの有効なリモートアクセスVPNユーザクレデンシャルを必要とします。

この脆弱性は、HTTPS POST要求のデータ検証が不適切であることに起因します。攻撃者は、巧妙に細工されたHTTPS POST要求を該当デバイスに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。エクスプロイトに成功すると、攻撃者はデバイスのリロードを引き起こし、その結果サービス妨害 (DoS) 状態に陥る危険性があります。

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。

このアドバイザリーは、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-dap-dos-bhEkP7n>

このアドバイザリーは、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ーバンドルの一部です。これらのアドバイザリー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](#)』

[アドバイザー公開半年刊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

この脆弱性は、Cisco ASAソフトウェアまたはCisco FTDソフトウェアの脆弱性が存在するリリースを実行するシスコ製品に影響を与え、次の条件すべてに当てはまります。

- SSL VPN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
- 少なくとも1つのカスタムDAPが設定されている
- ホストスキャンが有効です

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザーの「修正済みソフトウェア」セクションを参照してください。

SSL VPN 設定の確認

SSL VPNが有効になっているかどうかを確認するには、`show running-config webvpn | include ^ enable` コマンドをデバイスのCLIで使用します。次の例は、outsideインターフェイスでSSL VPNが有効になっているデバイスでの出力結果を示しています。

```
<#root>
firewall#
show running-config webvpn | include ^ enable

enable
  outside
```

空の出力は、どのインターフェイスでもSSL VPNが有効になっていないこと、およびデバイスがこの脆弱性の影響を受けないことを示します。

DAP 設定の確認

カスタムDAPが設定されているかどうかを確認するには、`show running-config dynamic-access-policy-record | exclude DfltAccessPolicy` コマンドをデバイスのCLIで実行する次に、TEST_POLICYという名前のカスタムDAPが設定されているデバイスでの出力例を示します。

```
<#root>
```

```
firewall#  
show running-config dynamic-access-policy-record | exclude DfltAccessPolicy  
  
dynamic-access-policy-record  
TEST_POLICY
```

空の出力は、カスタムDAPが設定されておらず、デバイスがこの脆弱性の影響を受けないことを示します。

ホストスキャン設定の確認

ホストスキャンが有効になっているかどうかを確認するには、`show running-config webvpn | include hostscan enable`コマンドを実行することによって確認できます。次の例は、ホストスキャンが有効になっているデバイスでの出力を示しています。

```
<#root>  
firewall#  
show running-config webvpn | include hostscan enable  
  
hostscan enable
```

空の出力は、ホストスキャンが有効になっていないこと、およびデバイスがこの脆弱性の影響を受けていないことを示します。

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 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャンネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアバージョンとフィーチャセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィーチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

Cisco.com の [シスコサポート & ダウンロードページ](#)には、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

[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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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
このアドバイザリのみ	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。

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 Advanced Security Initiatives Group (ASIG) の X.B. による内部セキュリティテストで発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dap-dos-bhEkP7n>

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、単独の転載や意識を施した場合、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。