# Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび 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-asa-ftd-dap-dos-GhYZBxDU
初公開日 : 2022-11-09 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwa47041

CVE-2022-20947

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）の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こし、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、ポスチャ（HostScan）モジュールから受信した HostScan データの不適切な処理に起因します。攻撃者は、該当デバイスに巧妙に細工された HostScan データを送信することにより、この脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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-asa-ftd-dap-dos-GhYZBxDU

このアドバイザリは、2022 年 11 月に公開された Cisco ASA、FTD、および FMC のセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、Cisco Event Response：2022 年 11 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（半期）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、次のすべての条件を満たしている、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しているシスコ製品に影響を与えます。

- リモートアクセス SSL VPN が有効になっている。
- HostScan が有効になっている。
- 少なくとも 1 つのカスタム DAP が設定されている。

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 と HostScan の設定の確認

show running-config webvpn | include enableコマンドをデバイスのCLIで実行して、リモートアクセスSSL VPN設定とHostScan設定を評価します。コマンドの出力に enable で始まる行が少なくとも 1 行含まれている場合、リモートアクセス SSL VPN が設定されています。コマンドの出力に hostscan enable がある行が含まれている場合、HostScan が設定されています。次に、外部インターフェイスでリモートアクセス SSL VPN が有効になっており、HostScan が有効になっているデバイスでの show running-config webvpn コマンドの出力の例を示します。

```
<#root>

asa#

show running-config webvpn | include enable

webvpn

enable

 outside

hostscan enable
```

このコマンドの出力が空の場合は、リモートアクセス SSL VPN も HostScan も設定されていないことを示しています。いずれかの行が欠落している場合、欠落している行の機能は設定されていません。

## DAP 設定の確認

デバイス CLI で show running-config dynamic-access-policy-record コマンドを使用して、DAP 設定を評価します。コマンドの出力に、DfltAccessPolicy レコードに加えて少なくとも 1 つのレコードが含まれている場合、カスタム DAP が設定されています。次に、DAP_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 show running-config dynamic-access-policy-record コマンドの出力例を示します。

```
<#root>

asa#

show running-config dynamic-access-policy-record


dynamic-access-policy-record DfltAccessPolicy

dynamic-access-policy-record

 DAP_TEST_POLICY
user-message "NO WAY IN!"
 action terminate
```

### 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。

シスコでは、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ています。

## 回避策

この脆弱性に対処する回避策はありません。ただし、管理者はデバイスのコンフィギュレーション モードで no hostscan enable コマンドを発行して、HostScan を無効にできます。

この緩和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

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ます。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 Cisco Support and Downloads 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 |
| このアドバイザのみ | Cisco ASA ソフトウェア | |
| あらゆるプラットフォーム | | |
| Enter Version | Check | |

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。

## 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-asa-ftd-dap-dos-GhYZBxDU

## 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 | 2022 年 11 月 9 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。