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 Web サービス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-websrvs-dos-X8gNucD2
初公開日 : 2024-04-24 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 : CSCwj10955

CVE-2024-20353

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）ソフトウェアの管理および VPN Web サーバーの脆弱性により、認証されていないリモートの攻撃者が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）状態が発生する可能性があります。

この脆弱性は、HTTP ヘッダーを解析する際のエラーチェックが不完全であることに起因します。攻撃者は、デバイス上のターゲット Web サーバーに巧妙に細工された HTTP リクエスト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。エクスプロイトが成功すると、デバイスのリロード中に DoS 状態が引き起こされ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-websrvs-dos-X8gNucD2

このアドバイザリに記載されている脆弱性の詳細については、『Cisco Event Response: Attacks Against Cisco Firewall Platforms』を参照してください。

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、次の 2 つの表に記載されている脆弱性のある設定を 1 つ以上含む Cisco ASA ソフトウェアおよび FTD ソフトウェアです。

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。

ASA または FTD デバイスが影響を受けるかどうかを判別する

Cisco ASA ソフトウェアまたは FTD ソフトウェアを実行中のデバイスが影響を受けるかどうかを判別するには、show asp table socket | include SSL コマンドを使用して、すべての TCP ポートの SSL リスニングソケットを検索します。出力にソケットが含まれている場合、そのデバイスは脆弱であると考えられます。TCP の 443 番ポートと TCP の 8443 番ポートで 2 つの SSL ソケットがリッスン状態になっている Cisco ASA デバイスの場合、出力は次のようになります。

```
<#root>

ciscoasa#

show asp table socket | include SSL


SSL       00185038  LISTEN     172.16.0.250:

443

    0.0.0.0:*
SSL       00188638  LISTEN      10.0.0.250:

8443

    0.0.0.0:*
```

ASA ソフトウェアにおける脆弱性のある設定

次の表の左側の列に、潜在的脆弱性のある Cisco ASA ソフトウェアの機能を示します。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSL リスニングソケットが有効になる可能性があります。

Cisco ASA ソフトウェアの機能	脆弱性の可能性がある設定
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）	crypto ikev2 enable [...] client-services port <port-number>
ローカル認証局（CA）[1]	crypto ca server no shutdown
管理 Web サーバーアクセス（ASDM および CSM を含む）[2]	http server enable http

Cisco ASA ソフトウェアの機能	脆弱性の可能性がある設定
モバイル ユーザ セキュリティ（MUS）	webvpn mus password mus server enable port mus
REST API[3]	rest-api image disk0:/rest-api agent
SSL VPN	webvpn enable

1. Cisco ASA ソフトウェアリリース 9.13 以降では、ローカル CA は廃止され、削除されています。
2. 管理 Web サーバーアクセスは、 http コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。
3. REST API は、 http コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。

FTD ソフトウェアにおける脆弱性のある設定

次の表の左側の列に、潜在的脆弱性のある Cisco FTD ソフトウェアの機能を示します。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSL リスニングソケットが有効になる可能性があります。

Cisco FTD ソフトウェアの機能	脆弱性の可能性がある設定
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）[1、2]	crypto ikev2 enable [...] client-services port <port-number>
AnyConnect SSL VPN[1、2]	webvpn enable
HTTP サーバー有効[3]	http server enable http

1. リモートアクセス VPN 機能は、Cisco Firepower Management Center（FMC）ソフトウェアで [デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）] の順に選択するか、Cisco Firepower Device Manager（FDM）で [デバイス（Devices）] > [リモートアクセス VPN（Remote Access VPN）] の順に選択すると有効になります。
2. リモートアクセス VPN 機能は、Cisco FTD ソフトウェアリリース 6.2.2 以降でサポートされています。
3. HTTP 機能は、Cisco FMC Console で [Firepower Threat Defenseプラットフォーム設定（Firepower Threat Defense Platform Settings）] > [HTTP] の順に選択すると有効になります。

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およびサービスのみが、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 FMC 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 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

シスコは、この脆弱性がエクスプロイトされたことを確認しました。この脆弱性を解消するため、修正済みのソフトウェアへのアップグレードを強く推奨します。また、システムログを監視して、文書化されていない設定変更、スケジュールされていない再起動、および異常なログインアクティビティの兆候がないかを確認することを強くお勧めします。

出典

今回の調査にご協力いただきました、次の機関に感謝申し上げます。

- オーストラリア信号局 Australian Cyber Security Centre
- Canadian Centre for Cyber Security（カナダ信安全保証部の機関）
- 英国 National Cyber Security Center（NCSC）
- 米国サイバーセキュリティ・インフラストラクチャ セキュリティ庁（CISA）

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

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 4 月 24 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。