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

High

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突発的に引き起こし、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不完全なエラーチェックに起因します。攻撃者は、デバイス上のターゲットWebサーバに巧妙に細工されたHTTP要求を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、デバイスのリロード時にDoS状態が引き起こされ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についての詳細は、『Ciscoイベントレスポンス：Ciscoファイアウォールプラットフォームに対する攻撃』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2つの表に記載されている脆弱性のある設定が1つ以上存在するCisco ASAソフトウェアおよびFTDソフトウェアに影響を与えます。

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デバイスが該当するかどうかの判別

Cisco ASAソフトウェアまたはFTDソフトウェアを実行しているデバイスが該当するかどうかを確認するには、show asp table socket | include SSLコマンドを使用して、任意の TCPポートのSSLリスニングソケットを探します。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。次の例は、TCPポート443とTCPポート8443に2つのSSLリスニングソケットがあるCisco ASAデバイスの出力を示しています。

```
<#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ソフトウェアの脆弱性のある設定

次の表では、左の列に脆弱性が存在する可能性のある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 <ポート番号>
ローカル認証局(CA)[1]	crypto ca server no shutdown
管理Webサーバアクセス（ASDMおよびCSMを含む）[2]	HTTPサーバ有効 http
モバイル ユーザ セキュリティ（MUS）	webvpn

Cisco ASA ソフトウェアの機能	脆弱性の可能性がある設定
	MUSパスワード MUSサーバのイネーブルポート mus
REST API[3]	rest-apiイメージdisk0:/rest-apiエージェント
SSL VPN（トンネルモード）	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は非推奨となり、削除されています。
2. 管理Webサーバアクセスは、 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. 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ソフトウェアの脆弱性のある設定

次の表では、左の列に、脆弱性が存在する可能性のある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 <ポート番号>
AnyConnect SSL VPN[1、2]	webvpn enable
HTTPサーバ有効[3]	HTTPサーバ有効 http

1. リモートアクセスVPN機能は、Cisco Firepower Management Center(FMC)ソフトウェアのDevices > VPN > Remote Access、またはCisco Firepower Device Manager(FDM)の Device > Remote Access VPNで有効になっています。
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からサポートされています。
3. HTTP機能は、Cisco FMCコンソールの Firepower Threat Defenseプラットフォームの設定> HTTPで有効になっています。

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に関するヘルプは、次の推奨リリースに関する文書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、この脆弱性が不正利用されたことを確認しました。この脆弱性を解決するには、修正済みソフトウェアにアップグレードすることを強く推奨します。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リブート、および異常なクレデンシャル情報のアクティビティを示すインジケータがないかどうかを確認することを強くお勧めします。

出典

シスコは、この調査をサポートしていただいた次の組織に感謝いたします。

- オーストラリア信号局のオーストラリアのサイバーセキュリティセンター
- カナダのサイバーセキュリティセンター、通信セキュリティ施設の一部
- 英国のNational Cyber Security Center(NCSC)
- 米国サイバーセキュリティおよびインフラストラクチャセキュリティ機関(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。