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 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-webdos-fBzM5Ynw
初公開日 : 2020-10-21 16:00
最終更新日 : 2020-10-23 01:06
バージョン 2.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvs10748 CSCvt70322

CVE-2020-3304

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

2020年10月22日からの更新：シスコは、このアドバイザリの「修正済みソフトウェア」セクションのコードトレイン9.13および9.14で推奨される修正済みリリースに影響を与える可能性がある、新しいCisco適応型セキュリティアプライアンスの脆弱性を認識しました。詳細については、Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSL/TLS におけるサービス妨害の脆弱性を参照してください。

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 Web インターフェイスの脆弱性により、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、HTTP リクエストの入力検証が適切に行われていないことに起因します。攻撃者は、該当デバイスに巧妙に細工された 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。攻撃者はエクスプロイトにより、DoS 状態を引き起こす可能性があります。

注：この脆弱性は、IPバージョン4(IPv4)およびIPバージョン6(IPv6)のHTTPトラフィックに適用されます。

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-webdos-fBzM5Ynw

このアドバイザリは、17 件の脆弱性に関する 17 件のシスコ セキュリティ アドバイザリを含む、2020 年 10 月に公開された Cisco ASA、FMC および FTD ソフトウェアのセキュリティ アドバイザリ バンドルの一部です。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: October 2020 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

この脆弱性の影響を受けるのは、シスコ製品で脆弱性のある Cisco ASA ソフトウェアまたは Cisco FTD ソフトウェアリリースを実行しており、HTTP 設定に脆弱性がある場合です。

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。

Cisco ASA ソフトウェア

次の表では、左列に脆弱性がある Cisco ASA ソフトウェアの機能を示します。右列には、show running-config CLI コマンドを実行すると表示される基本設定を示します。デバイスで脆弱性のあるソフトウェアリリースが実行されており、脆弱性のある機能が設定されている場合は、この脆弱性に影響を受けます。

Cisco ASA ソフトウェアの機能	脆弱性の存在するコンフィギュレーション
Adaptive Security Device Manager（ASDM）[1]	http server enable <port> http <remote_ip_address> <remote_subnet_mask> <interface_name>
Cisco Security Manager[1]	http server enable <port> http <remote_ip_address> <remote_subnet_mask> <interface_name>
REST API[2]	rest-api image disk0:/<image name> rest-api agent

1. ASDMおよびCisco Security Manager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。
2. REST APIは、Cisco ASAソフトウェアリリース9.3.2からサポートされています。

Cisco FTD ソフトウェア

次の表では、左列に、脆弱性がある Cisco FTD ソフトウェアの機能を示します。右列には、show running-config CLI コマンドを実行すると表示される基本設定を示します。デバイスで脆弱性のあるソフトウェアリリースが実行されており、脆弱性のある機能が設定されている場合は、この脆弱性に影響を受けます。

Cisco FTD ソフトウェアの機能	脆弱性の存在するコンフィギュレーション
HTTP サービス有効 [1]	http server enable <port #> http <remote_ip_address> <remote_subnet_mask> <interface_name>

1. HTTP機能は、Cisco Firepower Management Center(FMC)の Firepower Threat Defense(FTD)プラットフォーム設定> HTTPで有効になります。

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 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。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。

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。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。右の列は、リリースがこのバンドルに記載された何らかの脆弱性に該当するかどうか、およびそれらすべての脆弱性に対する修正を含む最初のリリースを示しています。

Cisco ASA ソフトウェア

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
9.6[1] より前	修正済みリリースに移行。	修正済みリリースに移行。
9.61	9.6.4.45	9.6.4.45
9.7[1]	修正済みリリースに移行。	修正済みリリースに移行。
9.8	9.8.4.22	9.8.4.29
9.9	9.9.2.80	9.9.2.80
9.10	9.10.1.44	9.10.1.44
9.12	9.12.3.12	9.12.4.4

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
9.13	9.13.1.12	9.13.1.13
9.14	9.14.1.10	9.14.1.30

1. Cisco ASAソフトウェアリリース9.7以前は、ソフトウェアメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
6.2.21 より前	修正済みリリースに移行。	修正済みリリースに移行。
6.2.2	修正済みリリースに移行。	修正済みリリースに移行。
6.2.3	修正済みリリースに移行。	修正済みリリースに移行。
6.3.0	6.3.0.6（リリース予定）	修正済みリリースに移行。
6.4.0	6.4.0.10	修正済みリリースに移行。
6.5.0	6.5.0.5（リリース予定）	修正済みリリースに移行。
6.6.0	6.6.1	6.6.1

1. Cisco FMC および FTD ソフトウェアリリース 6.0.1 以前および 6.2.0、6.2.1 については、ソフトウェアのメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

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-asaftd-webdos-fBzM5Ynw

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.0	[サマリー（Summary）] セクションを更新し、コードトレイン 9.13 および 9.14 に推奨される修正リリースに影響を与える新たな脆弱性の情報を入手してください。	要約	Final	2020-OCT-22
1.0	初回公開リリース	—	Final	2020 10月 21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。