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WebVPNポータルアクセスルールバイパスの脆弱性

アドバイザリーID : cisco-sa-asaftd-rule-bypass-P73ABNWQ
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 : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCvu75615

CVE-2020-3578

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サービスインターフェイスにおける脆弱性により、認証されていないリモートの攻撃者が、設定済みのアクセスルールをバイパスし、ブロックされるはずのWebVPNポータルの一部にアクセスする可能性があります。

この脆弱性は、ポータルアクセスルールが設定されている場合にURLの検証が不十分であることに起因します。攻撃者は、該当デバイスの特定のURLにアクセスすることで、この脆弱性を不正利用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-asaftd-rule-bypass-P73ABNWQ

該当製品

脆弱性のある製品

公開時点では、この脆弱性の影響を受けたシスコ製品は、脆弱性のあるAnyConnectまたはWebVPN設定を使用し、ポータルアクセスルールが設定されたCisco ASAソフトウェアまたはFTDソフトウェアの脆弱性のあるリリースを実行していました。

脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

ポータルアクセスルールが設定されているかどうかを確認する

ポータルアクセスルールが設定されているかどうかを確認するには、show running-config webvpn | include portal-access-ruleコマンドを使用します。このコマンドの出力が返された場合、デバイスに脆弱性が存在します。空の出力は、デバイスに脆弱性がないことを示します。

脆弱性のあるAnyConnectまたはWebVPN設定が存在するかどうかの確認

Cisco ASA ソフトウェア

次の表の左列は、脆弱性のある Cisco ASA 機能を示します。右列に示す Cisco ASA 機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。脆弱性のあるリリースがデバイスで実行されており、ここに示す機能のいずれかが設定されている場合は、脆弱性が存在します。

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
AnyConnect IKEv2 Remote Access (クライアント サービス有効時)	`crypto ikev2 enable <interface_name> client-services port <port #>`
AnyConnect SSL VPN	`webvpn` ` enable <interface_name>`
クライアントレス SSL VPN	`webvpn`

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
	webvpn enable <interface_name>

Cisco FTD ソフトウェア

次の表の左列は、脆弱性のある Cisco FTD 機能を示します。右列に示す Cisco ASA 機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。脆弱性のあるリリースがデバイスで実行されており、ここに示す機能のいずれかが設定されている場合は、脆弱性が存在します。

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
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）[1、2]	crypto ikev2 enable <interface_name> client-services port <port #>
AnyConnect SSL VPN[1、2]	webvpn enable <interface_name>

1. リモートアクセス VPN 機能は、Cisco Firepower Management Center（FMC）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、または 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からサポートされています。

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

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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右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の影響を受けるかどうか、およびこの脆弱性に対する修正を含む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
9.6[1] より前	修正済みリリースに移行。
9.61	9.6.4.45
9.7[1]	修正済みリリースに移行。
9.8	9.8.4.26
9.9	9.9.2.80
9.10	9.10.1.44
9.12	9.12.4.4
9.13	9.13.1.13
9.14	9.14.1.19

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
6.2.21 より前	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。
6.2.3	修正済みリリースに移行。
6.3.0	6.3.0.6（リリース予定）
6.4.0	6.4.0.10
6.5.0	6.5.0.5（リリース予定）
6.6.0	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-rule-bypass-P73ABNWQ

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。