Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defense(FTD)ソフトウェアのVPN Webクライアントサービスのクライアント側の要求密輸の脆弱性

アドバイザリーID : cisco-sa-asa-webvpn-LOeKsNmO
CVE-2022-20713
初公開日 : 2022-08-10 16:00
最終更新日 : 2023-11-01 16:00
バージョン 3.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwa04262 CSCwe93561 CSCwf47924 CSCwd95043

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VPN Webクライアントサービスコンポーネントの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのユーザに対してブラウザベースの攻撃を行う可能性があります。

この脆弱性は、VPN Web Clientサービスコンポーネントに渡された入力が、使用中のブラウザに返される前に不適切に検証されることに起因します。攻撃者は、Cisco ASAソフトウェアまたはCisco FTDソフトウェアを実行し、VPN機能をサポートするWebサービスエンドポイントが有効になっているデバイスに悪意のある要求を送信するように設計されているWebサイトにユーザを誘導することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は影響を受けるデバイスから使用中のブラウザに悪意のある入力を反映させ、クロスサイトスクリプティング攻撃などのブラウザベースの攻撃を実行する可能性があります。攻撃者は、影響を受けるデバイスに直接影響を及ぼすことはできません。

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-webvpn-LOeKsNmO

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、次のシスコソフトウェアの脆弱性のあるリリースを実行しているシスコ製品に影響を与えました。

- Cisco AnyConnect VPNまたはクライアントレスSSL VPNが有効なASAソフトウェア
- Cisco AnyConnect VPNが有効なFTDソフトウェア

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。

ASA ソフトウェア設定の確認

脆弱性のある機能がソフトウェアで有効になっているかどうかを確認するには、show-running-config CLIコマンドを使用します。次の表の左列は、脆弱性のある Cisco ASA 機能を示します。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。デバイスが脆弱なリリースを実行しており、これらの機能のいずれかが有効になっている場合、そのデバイスは脆弱です。

Cisco ASA 機能	脆弱性の存在するコンフィギュレーション
AnyConnect インターネット キー エクスチェンジ バージョン 2 リモートアクセス (クライアントサービス有効時)	`crypto ikev2 enable client-services port`
AnyConnect SSL VPN	`webvpn` ` enable`
クライアントレス SSL VPN	`webvpn` ` enable`

FTD ソフトウェア設定の確認

脆弱性のある機能がソフトウェアで有効になっているかどうかを確認するには、show-

running-config CLIコマンドを使用します。次の表の左列は、脆弱性のある Cisco FTD 機能を示します。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。デバイスが脆弱なリリースを実行しており、これらの機能のいずれかが有効になっている場合、そのデバイスは脆弱です。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
AnyConnect インターネット キー エクスチェンジ バージョン 2 リモートアクセス（クライアントサービス有効時）[1、2]	`crypto ikev2 enable  client-services port`
AnyConnect SSL VPN[1、2]	`webvpn` `enable`

1. 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 で導入されました。
2. 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。

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、クライアントサービスが無効にされたAnyConnect Internet Key Exchange（IKE；インターネットキーエクスチェンジ）バージョン2リモートアクセスVPNのみを受け入れるように設定されたリモートアクセスVPNサービスを持つデバイスが、この脆弱性の影響を受け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。

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	

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

この脆弱性を報告していただいたPortswigger.netのJames Kettle氏に感謝いたします。

また、この脆弱性に関する追加の詳細を報告していただいたNoZero社のValerio Brussani氏にも感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-webvpn-LOeKsNmO

改訂履歴

バージョン	説明	セクション	ステータス	日付
3.0	Cisco ASAソフトウェアとFTDソフトウェアの修正を追加し、ソースを更新。	修正済みソフトウェアとソース	Final	2023 年 11 月 1 日
2.1	修正済みソフトウェアの入手可能性に関する情報を更新。	修正済みソフトウェアの概要	Final	2022-DEC-16
2.0	該当製品としてFTDソフトウェアを追加。影響を受けるVPNコンポーネントを更新。影響を受けるソフトウェア構成を明確化。適用されなくなったため、緩和策を削除しました。	タイトル、概要、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品、回避策	Final	2022 年 11 月 9 日
1.0	初回公開リリース	—	Final	2022 年 8 月 10 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。