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 サービスの読み取り専用パストラバーサルの脆弱性

アドバイザリーID : cisco-sa-asaftd-ro-path-KJuQhB86
CVE-2020-3452
初公開日 : 2020-07-22 16:00
最終更新日 : 2020-08-27 14:33
バージョン 1.5 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCvt03598

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 Web サービス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ディレクトリトラバーサル攻撃を仕掛け、ターゲットシステムの機密ファイル読み取る可能性があります。

この脆弱性は、影響を受けるデバイスで処理される HTTP リクエスト内の URL の入力検証が適切でないことに起因します。攻撃者は、ディレクトリトラバーサルの文字列を含むように細工された HTTP リクエストを影響を受けるデバイスに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。エクスプロイトに成功すると、攻撃者はターゲットデバイス上の Web サービスファイルシステム内にある任意のファイルを表示できます。たとえば、別の VPN ユーザになりすまして、デバイスへのクライアントレス SSL VPN や AnyConnect VPN セッションを確立することがが可能になります。

影響を受けるデバイスに WebVPN または AnyConnect 機能が設定されている場合、Web サービスファイルシステムが有効になっています。この脆弱性を利用して、ASA や FTD システムファイル、基盤となるオペレーティングシステム (OS) のファイル、または VPN ユーザのログインクレデンシャルにアクセスすることはできません。

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。

注：シスコは、このアドバイザリに記載されている公開悪用コードが使用可能で、脆弱性が活発に悪用されていることを認識しています。シスコでは、影響を受ける製品をお持ちのお客様には、できるだけ早く修正済みリリースにアップグレードすることを推奨しています。

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-ro-path-KJuQhB86

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、かつ脆弱な AnyConnect または WebVPN が設定されている場合です。

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。ここに示す機能のいずれかがデバイスに設定されている場合は、脆弱性が存在します。

Cisco ASA 機能	脆弱性の存在するコンフィギュレーション
AnyConnect 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` ` enable <interface_name>`

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。ここに示す機能のいずれかがデバイスに設定されている場合は、脆弱性が存在します。

Cisco FTD ソフトウェアを実行しているデバイスでは、診断 CLI モードからのみ show running-config コマンドを実行できます。診断 CLI モードを開始するには、通常の Firepower Threat Defense CLI で system support diagnostic-cli コマンドを使用します。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
AnyConnect 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)の デバイス> VPN > Remote Access、またはCisco Firepower Device Manager(FDM)の デバイス> Remote Access VPNを介して有効になります。
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。

詳細

攻撃者は、Web サービスファイルシステム内にあるファイルのみ表示できます。Webサービスファイルシステムは、このアドバイザリの「脆弱性のある製品」の項に記載されているWebVPNおよびAnyConnect機能に対して有効です。したがって、この脆弱性はASAおよびFTDシステムファイル、または基盤となるオペレーティングシステム(OS)ファイルには適用されません。攻撃者が表示できる Web サービスファイルには、WebVPN 設定、ブックマーク、Web クッキー、 Web コンテンツの一部、HTTP URL などの情報が保存されている可能性があります。

回避策

この脆弱性に対処する回避策はありません。

このアドバイザリに記載されている脆弱性をエクスプロイトする試みを検出またはブロックするために、Cisco Firepower センサー上の影響を受けるトラフィックに対して SSL 復号化機能を使用するお客様は、Cisco Firepower Management Center を使用して、SRU 番号 2020-07-22-001 から、Snort ルール 54598 ～ 54601 を有効にできます。

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。右側の列は、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ているかどうか、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。

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。
9.6	9.6.4.42
9.7[1]	修正済みリリースに移行。
9.8	9.8.4.20
9.9	9.9.2.74
9.10	9.10.1.42
9.12	9.12.3.12
9.13	9.13.1.10
9.14	9.14.1.10

1. Cisco ASA ソフトウェアリリース 9.5 以前および 9.7 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

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
6.2.2 より前	脆弱性なし
6.2.2	修正済みリリースに移行。
6.2.3	6.2.3.16
6.3.0	6.4.0.9 + ホットフィックスまたは 6.6.0.1 への移行 または 6.3.0.5 + ホットフィックス [1] または 6.3.0.6（2020 年秋）
6.4.0	6.4.0.9 + ホットフィックス [1] または 6.4.0.10（2020 年秋）
6.5.0	6.6.0.1 に移行 または 6.5.0.4 + ホットフィックス [1] または 6.5.0.5（2020 年秋）

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
6.6.0	6.6.0.1

1.ホットフィックスの詳細については、次の表を参照してください。

Cisco FTD ソフトウェアのホットフィックスの詳細

Cisco FTD ソフトウェア リリース	ホットフィックスファイル名
6.3.0.5	Cisco_FTD_Hotfix_AV-6.3.0.6-3.sh.RE L.tar Cisco_FTD_SSP_Hotfix_AV-6.3.0.6-3.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_AV-6.3.0.6-3.sh.RE L.tar
6.4.0.9	Cisco_FTD_Hotfix_BM-6.4.0.10-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2.sh.RE L.tar
6.5.0.4	Cisco_FTD_Hotfix_O-6.5.0.5-3.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_O-6.5.0.5-3.sh.RE L.tar Cisco_FTD_SSP_Hotfix_O-6.5.0.5-3.sh.RE L.tar

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; プロダクト セキュリティ インシデント レスポンス チーム）では、本アドバイザリに記載されている脆弱性の公開エクスプロイトコードが存在することと、エクスプロイトが実行可能であることを認識しています。

出典

この脆弱性を個別にご報告いただいた Positive Technologies 社の Mikhail Klyuchnikov 氏、および RedForce 社の Abdulrahman Nour と Ahmed Aboul-Ela 氏に対して、ここに感謝の意を表します。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.5	VPNユーザログインクレデンシャルが公開されないことを明確にし、修正済みソフトウェアの可用性を更新。	修正済みソフトウェアの概要	Final	2020 年 8 月 27 日
1.4	潜在的な影響に関する詳細を追記。	要約	Final	2020 年 7 月 28 日
1.3	リスク緩和に関する詳細を追加。	回避策	Final	2020 年 7 月 23 日
1.2	アクティブなエクスプロイトについて警告するために更新。	サマリ、不正利用事例と公式発表	Final	2020 年 7 月 23 日
1.1	公開エクスプロイトコードの可用性を示すために更新。	不正利用事例と公式発表	Final	2020 年 7 月 23 日
1.0	初回公開リリース	—	Final	2020 年 7 月 22 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。