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 サービスで確認された情報開示の脆弱性

High

アドバイザリーID : cisco-sa-asaftd-info-disclose-9eJtycMB
初公開日 : 2020-05-06 16:00
最終更新日 : 2024-02-21 15:57
バージョン 1.5 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCvt15163

CVE-2020-3259

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で脆弱性が確認されました。認証されていないリモートの攻撃者が、該当デバイスでメモリの内容を搾取し、機密情報を開示する可能性があります 。

この脆弱性は、ソフトウェアが Web サービスインターフェイスから要求された無効な URL を解析する際のバッファトラッキングに問題があることに起因します。細工された GET 要求が Web サービスインターフェイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、メモリの内容を搾取できるようになり、機密情報の漏洩につながる可能性があります。

注：この脆弱性の影響を受けるのは、特定のAnyConnectおよびWebVPN設定のみです。詳細については、「脆弱性のある製品」のセクションを参照してください。

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-info-disclose-9eJtycMB

このアドバイザリは、2020 年 5 月 に公開された Cisco ASA、FMC、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。このアドバイザリバンドルには、12 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。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: May 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 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。

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 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。

詳細

開示される可能性のある機密情報は、システムヒープ上のメモリです。このメモリの内容はシステムや時間によって異なりますが、AnyConnect と WebVPN の機能、ユーザ名、電子メールアドレス、証明書、および実際のヒープアドレスの Web クッキーが含まれ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。

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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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
9.5[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。
9.51	修正済みリリースに移行。	修正済みリリースに移行。
9.6	9.6.4.41	修正済みリリースに移行。
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	9.8.4.20	9.8.4.20
9.9	9.9.2.67	9.9.2.67
9.10	9.10.1.40	9.10.1.40
9.12	9.12.3.9	9.12.3.9

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	9.13.1.10	9.13.1.10
9.14	脆弱性なし	脆弱性なし

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	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
6.2.3[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。
6.2.3	6.2.3.16（2020 年 6 月） Cisco_FTD_Hotfix_DT-6.2.3.16-3.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3.sh.REL.tar Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3.sh.REL.tar	6.2.3.16（2020 年 6 月） Cisco_FTD_Hotfix_DT-6.2.3.16-3.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3.sh.REL.tar Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3.sh.REL.tar
6.3.0	6.3.0.6（リリース予定） Cisco_FTD_Hotfix_AO-6.3.0.6-2.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2.sh.REL.tar Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2.sh.REL.tar	6.3.0.6（リリース予定） Cisco_FTD_Hotfix_AO-6.3.0.6-2.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2.sh.REL.tar Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2.sh.REL.tar
6.4.0	6.4.0.9	6.4.0.9
6.5.0	6.5.0.5（リリース予定） Cisco_FTD_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降	6.5.0.5（リリース予定） Cisco_FTD_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降

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
6.6.0	脆弱性なし	6.6.0

1. Cisco FMC および FTD ソフトウェア リリース 6.0.1 以前については、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

2024年2月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性の不正利用が試みられたという情報を入手しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性をご報告いただいた Positive Technologies 社の Mikhail Klyuchnikov 氏と Nikita Abramov 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-info-disclose-9eJtycMB

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	不正利用事例と公式発表の更新	不正利用事例と公式発表	Final	2024年2月21日

バージョン	説明	セクション	ステータス	日付
1.4	修正済み FTD リリース 6.4.0 ソフトウェアのリリースに関する情報を更新。	修正済みリリース	Final	2020年6月2日
1.3	FTD リリース 6.4.0 および 6.5.0 の Hot Fix を更新。	修正済みリリース	Final	2020 年 5 月 15 日
1.2	9.6 リリースで ASA 修正済みリリースの表を更新。	修正済みソフトウェア	Final	2020 年 11 月
1.1	正しい修正済みリリースを 9.10.1.39 ではなく 9.10.1.40 とするために、ASA 修正リリーステーブルを更新。	修正済みソフトウェア	Final	2020 年 5 月 6 日
1.0	初回公開リリース	—	Final	2020 年 5 月 6 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。