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 Firepower Threat Defense ソフトウェア WebVPN クロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190501-asa-ftd-xss **初公開日 :** 2019-05-01 16:00 **最終更新日 :** 2019-05-02 17:42 **バージョン 1.1 :** Final **CVSSスコア :** 4.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvo17033 CSCvo11406 CSCvo11416 CSCvn78674	CVE-2019-1701

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 WebVPN サービスの多重 脆弱点は影響を受けたデバイスの WebVPN ポータルのユーザに対してクロスサイト スクリプティング（XSS）攻撃を行なう認証される、リモート攻撃者可能にする可能性があります。

脆弱性はソフトウェアが不十分に影響を受けたデバイスのユーザが指定する入力を検証するのであります。 攻撃者はインターフェイスのユーザの巧妙に細工された リンクをクリックするように説得によってこれらの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が任意スクリプト コードを影響を受けたインターフェイスという点において実行するか、または敏感なブラウザ ベースの情報にアクセスすることを可能にする可能性があります。 攻撃者はデバイスの*アドミニストレーター特権*をこれらの脆弱性を不正利用する必要とします。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これら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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-

xss

該当製品

脆弱性のある製品

これらの脆弱性は Cisco ASA ソフトウェアまたは FTD ソフトウェアの脆弱なリリースを実行して、有効に なる WebVPN サービスがある以下のシスコ製品に影響を及ぼします:

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- ASA 1000V クラウド ファイアウォール
- ASA 5500-X シリーズ ファイアウォール
- ASA 5505 適応型セキュリティ アプライアンス[1]
- Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の ASA サービス モジュール
- 適応型セキュリティ仮想アプライアンス（ASAv）
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- FTD Virtual（FTDv）

ASA 5505 以外の [1]ASA 5500 シリーズは適応型セキュリティ アプライアンス（ASA）サポート終了マイルストーンに達し、セキュリティーの脆弱性のためにもはや評価されます。

情報に関しては Cisco どのについての ASA ソフトウェアおよび FTD ソフトウェア リリース脆弱 でであって下さいか、このアドバイザリの修正済みソフトウェアのセクションを参照して下さい。

Cisco ASA ソフトウェア リリースの判別

Cisco どの ASA ソフトウェア リリースがデバイスで動作しているか判別するために、管理者はデバイスにログイン、**show version を**使用するためにできます **| Version コマンドを** CLI に **含め**、コマンドの出力を参照して下さい。 次の例は Cisco ASA ソフトウェア リリース 9.9.2.18 を実行しているデバイスのためのコマンドの出力を示したものです:

```
ciscoasa# show version | include Version
Cisco Adaptive Security Appliance Software Version 9.9.2.18
Device Manager Version 7.4(1)
.
.
.
```

デバイスが Cisco Adaptive Security Device Manager（ASDM）を使用して管理されている場合、管理者は Cisco ASDM ログイン ウィンドウまたは [Cisco ASDM ホーム（Cisco ASDM Home）] ペインの [デバイス ダッシュボード（Device Dashboard）] タブに表示される表のリ

リース情報を参照して、デバイスで実行中のリリースを確認することもできます。

Cisco FTD ソフトウェア リリースの判別

デバイスで実行中の Cisco FTD ソフトウェア リリースを確認するために、管理者はデバイスにログインし、CLI で **show version** コマンドを使用してコマンドの出力を参照できます。 デバイスが Cisco FTD ソフトウェア リリース 6.2.0 を実行している場合、コマンドの出力例は次のようになります。

```
> show version

--------------------[ ftd ]--------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.0 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
-----------------------------------------------------
```

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、これらの脆弱性の影響を受けることが分かっています。

回避策

これら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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。
次のテーブルでは、左カラムは Ciscoソフトウェアリリースをリストします。 右の列はリリースがこれらの脆弱性のための修正が含まれているリリースおよびこのアドバイザリに説明がある脆弱性から影響を受けするかどうか示します。

Cisco ASA ソフトウェア

Cisco ASA ソフトウェア リリース	これらの脆弱性のための推奨されるリリース
9.4[1] 前	9.4.4.34
9.4	9.4.4.34
9.5[1]	9.6.4.25
9.6	9.6.4.25
9.7[1]	9.8.4
9.8	9.8.4
9.9	9.9.2.50
9.10	9.10.1.17
9.12	脆弱性なし

リリース 9.4 以前の [1Cisco] ASA ソフトウェア リリースおよび Cisco ASA ソフトウェア リリース 9.5 および 9.7 はメンテナンスの終わりに達しました。 顧客はこれらの脆弱性のための修正を含むサポートされているリリースに移行する必要があります。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	これらの脆弱性のための推奨されるリリース
6.0	脆弱性なし

6.0.1	脆弱性なし
6.1.0	脆弱性なし
6.2.0	脆弱性なし
6.2.1	6.2.3.12
6.2.2	6.2.3.12
6.2.3	6.2.3.12
6.3.0	6.3.0.3
6.4.0	脆弱性なし

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ために、顧客は次のいずれかの操作を行うことができます:

- Cisco Firepower Management Center （ FMC ）の使用によって管理されるデバイスに関しては、アップグレードをインストールするのに FMC インターフェイスを使用して下さい。 インストールが完了する後、アクセスコントロール ポリシーを再適用して下さい。
- Cisco Firepower デバイスマネージャ（ FDM ）の使用によって管理されるデバイスに関しては、アップグレードをインストールするのに FDM インターフェイスを使用して下さい。 インストールが完了する後、アクセスコントロール ポリシーを再適用して下さい。

不正利用事例と公式発表

Cisco Product Security Incident Response Team （ PSIRT ）では、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とその公表は確認しておりません。

出典

Cisco はこれらの脆弱性の 1 報告するために Qihoo 360 情報 セキュリティ部のチエン陳に感謝することを望みます。 このアドバイザリの他の脆弱性は内部 保全テストの間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-xss

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	FTD 修正済みリソース 表を FTD ソフトウェア リリース 6.3.0.3 が利用できることを示すために更新しました。	修正済みソフトウェア	最終版	2019-May-02
1.0	初回公開リリース		最終版	2019-May-01

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。