Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア アクセス制御リスト バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20181003-asa-acl-bypass **初公開日 :** 2018-10-03 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvj91858	CVE-2018-15398

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）ソフトウェアの毎ユーザ上書きする 機能の脆弱性は影響を受けたデバイスのインターフェイスのために設定されるリモート攻撃者非認証が Access Control List（ACL）をバイパスするようにする可能性があります。

脆弱性は影響を受けたソフトウェアが毎ユーザ上書きするルールを組み立て、適用するとき生じる可能性があるエラーが原因です。 攻撃者は脆弱 な 設定がある影響を受けたデバイスを通ってネットワークに接続によってこ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影響を受けたデバイスの後ろに攻撃者がリソースにアクセスすることを可能にするある可能性があり、インターフェイス ACL によって一般的に保護されます。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-asa-acl-bypass

該当製品

脆弱性のある製品

この脆弱性は Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアまたは Cisco Firepower Threat Defense（FTD）ソフトウェアの脆弱なリリースを実行して、すべての次の状態を満たすシスコ製品に影響を及ぼします:

- 少なくとも 1 つのインターフェイス ACL に有効に なる毎ユーザ上書きする 機能（毎ユーザ**上書きする**）があります。
- 少なくとも 1 つのリモートアクセスVPN接続 プロファイルかサイト間VPN 接続プロファイル（**トンネル グループ**）はフィルタ ACL（VPN **フィルタ**）を規定 するグループ ポリシー（**グループ ポリシー**）と設定され、関連付けられます。
- VPN トンネルは影響を受けた接続プロファイル（**トンネル グループ**）と関連付けられる現在あります。

注: Cisco FTD ソフトウェアでは、毎ユーザ上書きする 機能は FlexConfig だけによって有効にすることができます。

該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

Cisco ASA ソフトウェア リリースを判別して下さい

、管理者はデバイスにログイン 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し、**show version コマンドを** CLI で使用し、コマンドの出力を参照するためにできます。 デバイスが Cisco ASA ソフトウェア リリース 9.4(4) を実行している場合は、コマンドの出力は次のようになります。

```
ciscoasa#  show version | include Version

Cisco Adaptive Security Appliance Software Version 9.4(4)
Device Manager Version 7.4(1)
.
.
.
```

デバイスが Cisco Adaptive Security Device Manager（ASDM）の使用によって管理されれば、管理者はまたどのリリースがデバイスで Cisco ASDM ホーム ペインの Cisco ASDM Log In ウィンドウか**デバイス ダッシュボード** タブに現われる表かのリリース情報を示すことによって動作しているか判別できます。

Cisco FTD ソフトウェア リリースを判別して下さい

、管理者はデバイスにログイン Cisco どの FTD 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し、**show version コマンドを** CLI で使用し、コマンドの出力を参照するためにできます。 次の例は Cisco FTD ソフトウェア リリース 6.2.0 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:

```
> 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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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。

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エクスプロイト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 のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-asa-acl-bypass

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-03

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。