Cisco Firepower Threat Defense ソフトウェアの FTP インスペクションにおけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20181003-ftd-inspect-dos

初公開日 : 2018-10-03 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvh77456

CVE-2018-15390

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 Firepower Threat Defense（FTD）ソフトウェアの FTP インスペクション エンジンの脆弱性により、認証されていないリモートの攻撃者が影響を受けるデバイスのリロードを引き起こし、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、ソフトウェアが中継トラフィックに FTP インスペクションとアクセス制御ルールを適用するように設定されていて、そのアクセス制御ルールが FTP ファイル ポリシーと関連付けられている場合、デバイスがシステム メモリが不足した状態で動作しているときに、影響を受けるソフトウェアがスピンロックのリリースに失敗するために存在します。 攻撃者は、影響を受けるデバイスを介して高いレートの中継トラフィックを送信し、デバイスをメモリ不足状態にすることで、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した攻撃者は、影響を受けるデバイスでソフトウェア パニックを引き起こし、デバイスがリロードされて一時的に DoS 状態になる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-ftd-inspect-dos

該当製品

脆弱性のある製品

この脆弱性は、FTP インスペクションが有効になっている、関連する FTP ファイル ポリシーのアクセス制御ルールも有効になっていて、ソフトウェアが次のシスコ製品で実行されている場合、リリース 6.2.3.4 より前の Cisco Firepower Threat Defense（FTD）ソフトウェア リリース 6.2.3.x 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）
- Cisco ASA 5500-X シリーズ次世代ファイアウォール製品群
- FirePOWER 2100 シリーズ セキュリティ アプライアンス
- FirePOWER 4100 シリーズ セキュリティ アプライアンス
- FirePOWER 9300 ASA セキュリティ モジュール
- Firepower Threat Defense Virtual（FTDv）

FTP インスペクションは、Cisco FTD ソフトウェアではデフォルトで有効になっています。アプリケーション インスペクション ポリシーのデフォルト設定の詳細については、Cisco ASA Series Firewall CLI Configuration Guide を参照してください。

Cisco FTD ソフトウェア リリースの確認

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
-------------------------------------------------
```

FTP ファイル ポリシーがルールと関連付けられているかどうかの確認

FTP ファイル ポリシーがデバイスに対して有効になっているアクセス制御ルールと関連付けられているかどうかを確認するために、管理者は次のいずれかを実行できます。

- Cisco Firepower Management Center（FMC）を使用して管理されているデバイスの場合は、Cisco FMC を開き、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択し、アクセス制御ルールを選択します。[ファイル ポリシー（File Policy）] タブをクリックして、ルールと関連付けられているファイル ポリシーに関する詳細を確認します。
- Cisco Firepower Device Manager（FMC）を使用して管理されているデバイスの場合は、Cisco FMC を開き、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択し

、アクセス制御ルールを選択します。 [ファイル ポリシー（File Policy）] タブをクリックして、ルールと関連付けられているファイル ポリシーに関する詳細を確認します。 Cisco FDM では定義済みのファイル ポリシーの使用のみサポートされる点に注意してください。 管理者はアクセス制御ルールのファイル ポリシーを作成できません。

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。

シスコでは、この脆弱性が Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアに影響を及ぼさないことを確認しています。

回避策

この脆弱性に対処する回避策はありません。 ただし、管理者は FTP インスペクションを無効化できます。 Cisco FTD ソフトウェア リリース 6.2 以降で FTP インスペクションを無効化するには、Cisco FMC を使用して次の FlexConfig ポリシーを追加します。

```
policy-map global_policy
 class inspection_default
 no inspect ftp
```

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 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。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20181003-asa-dma-dos： Cisco 適応型セキュリティ アプライアンス（ASA）のダイレクト メモリ アクセスにおけるサービス妨害（DoS）の脆弱性
- cisco-sa-20181003-ftd-inspect-dos： Cisco Firepower Threat Defense ソフトウェアの FTP インスペクションにおけるサービス妨害（DoS）の脆弱性

次の表では、左の列にシスコ ソフトウェアのリリースを示しています。 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、リリースがこのアドバイザリ集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 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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	脆弱性なし	6.1.0.7 への移行が必要
6.0.1	脆弱性なし	6.1.0.7 への移行が必要
6.1.0	脆弱性なし	6.1.0.7
6.2.0	脆弱性なし	6.2.0.7（リリース予定）
6.2.1	脆弱性なし	6.2.2.5（リリース予定）への移行が必要
6.2.2	脆弱性なし	6.2.2.5（リリース予定）
6.2.3	6.2.3.4 6.2.3-85[1] 6.2.3-991[2]	6.2.3.4 6.2.3-85[1] 6.2.3-991[2]

[1] AWS Cloud 用の Cisco Firepower Threat Defense Virtual（FTDv）のソフトウェア イメージ。
[2] Microsoft Azure Cloud 用の Cisco FTDv のソフトウェア イメージ。

Cisco FirePOWER システム 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、次のいずれかの操作を実行できます。

- 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、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。 インストールされている Snort バージョンは、FMC リリースによって異なります。
- Cisco Adaptive Security Device Manager（ASDM）または 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、ASDM または 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、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）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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-ftd-inspect-dos

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 10 月 3 日

利用規約