# 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

High

**アドバイザリーID :** cisco-sa-20181003-asa-dma-dos

**初公開日 :** 2018-10-03 16:00

**最終更新日 :** 2018-10-29 14:02

**バージョン 1.1 :** Final

**CVSSスコア :** 8.6

**回避策 :** No workarounds available

**Cisco バグ ID :** CSCvj89470

CVE-2018-15383

**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）ソフトウェアの暗号ハードウェア アクセラレータ ドライバの脆弱性により、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、影響を受けるデバイスのダイレクト メモリ アクセス（DMA）メモリの量が限られていて、影響を受けるソフトウェアによるメモリ不足状態時のリソースの処理が適切でないために存在します。 攻撃者は、影響を受けるデバイスに悪意のあるトラフィックを継続的に高いレートで送信し、デバイス上のメモリを使い果たすことで、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が、影響を受けるデバイスの DMA メモリを使い果たし、それにより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。

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ました。 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-dma-dos

## 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性があるリリースを実行している次のシスコ製品に影響を及ぼします。

- ASA 5506-X with FirePOWER サービス
- ASA 5506H-X with FirePOWER サービス
- ASA 5506W-X with FirePOWER サービス
- ASA 5508-X with FirePOWER サービス
- ASA 5516-X with FirePOWER サービス

この脆弱性は、FirePOWER サービスがインストールされていないか、または有効になっている場合、上記の製品にも影響を及ぼします。

脆弱性が存在する Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

## Cisco ASA ソフトウェア リリースの確認

デバイスで実行中の Cisco ASA 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 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）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
-----------------------------------------------------
```

## 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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 7600 シリーズ 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）
- ASA 1000V クラウド ファイアウォール
- ASA 5512-X with FirePOWER サービス
- ASA 5515-X with FirePOWER サービス
- ASA 5525-X with FirePOWER サービス
- ASA 5545-X with FirePOWER サービス
- ASA 5555-X with FirePOWER サービス
- ASA 5585-X with FirePOWER SSP-10、SSP-20、SSP-40、または SSP-60
- ASA 5505 適応型セキュリティ アプライアンス
- ASA 5510 適応型セキュリティ アプライアンス
- ASA 5512-X 適応型セキュリティ アプライアンス
- ASA 5515-X 適応型セキュリティ アプライアンス
- ASA 5520 適応型セキュリティ アプライアンス
- ASA 5525-X 適応型セキュリティ アプライアンス
- ASA 5540 適応型セキュリティ アプライアンス
- ASA 5545-X 適応型セキュリティ アプライアンス
- ASA 5550 適応型セキュリティ アプライアンス
- ASA 5555-X 適応型セキュリティ アプライアンス
- ASA 5580 適応型セキュリティ アプライアンス
- ASA 5585-X 適応型セキュリティ アプライアンス
- Catalyst 6500 シリーズ ASA サービス モジュール
- 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 7000 シリーズ アプライアンス
- FirePOWER 8000 シリーズ 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）

# 詳細

このアドバイサリに記載されている脆弱性は、影響を受けるデバイスの DMA メモリの量が限られていて、影響を受けるソフトウェアによるメモリ不足状態時のリソースの処理が適切でないために存在します。 影響を受けるソフトウェアが DMA メモリを割り当てられない場合、デバイスのクラッシュとリロードを引き起こし、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ために、シスコはソフトウェアによるメモリ不足状態時のリソースの処理方法を修正しました。 また、デバイスで DMA メモリ割り当てエラーが発生しているかどうか、およびエラー発生回数を確認するために管理者が使用できる DMA_MEM_ALLOC_FAILED プロトコル スタック カウンタも実装しました。 長期間の DMA メモリ割り当てエラーは、デバイスを介して送信されるトラフィックに悪影響を与える可能性があります。

DMA_MEM_ALLOC_FAILED カウンタの値を確認するために、管理者は次の例のように、デバイスの CLI で **show counters** 特権 EXEC コマンドを使用できます。

```
ciscoasa# show counters

Protocol      Counter                                         Value    Context
.
.
.
CRYPTO      DMA_MEM_ALLOC_FAILED                    1   Summary
```

DMA_MEM_ALLOC_FAILED カウンタの値が長期間急激に増加している場合、管理者は Cisco Technical Assistance Center（TAC）にさらなる調査を依頼する必要があります。

# 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。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 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 | First Fixed Release for All Vulnerabilities Described in the Collection of Advisories |
|---|---|---|

| | | |
|---|---|---|
| 9.1[1] 前 | 脆弱性なし[2] | 脆弱性なし[2] |
| 9.1 | 脆弱性なし[2] | 脆弱性なし[2] |
| 9.2[1] | 脆弱性なし[2] | 脆弱性なし[2] |
| 9.3[1] | 9.4.4.22 への移行が必要 | 9.4.4.22 への移行が必要 |
| 9.4 | 9.4.4.22 | 9.4.4.22 |
| 9.5[1] | 9.6.4.14 への移行が必要 | 9.6.4.14 への移行が必要 |
| 9.6 | 9.6.4.14 | 9.6.4.14 |
| 9.7[1] | 9.8.3.8 への移行が必要 | 9.8.3.8 への移行が必要 |
| 9.8 | 9.8.3.8 | 9.8.3.8 |
| 9.9 | 9.9.2.18 | 9.9.2.18 |

[1] Cisco ASA ソフトウェアの 9.1 より前のリリース、Cisco ASA ソフトウェア リリース 9.2、9.3、9.5、および 9.7 については、ソフトウェア メンテナンスのマイルストーンが終了しています。 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。

[2] Cisco ASA ソフトウェアの 9.3 より前のリリースは、Cisco ASA 5506-X、5506H-X、5506W-X、5508-X、および 5516-X アプライアンスではサポートされていません。

### 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 | First Fixed Release for All Vulnerabilities Described in the Collection of Advisories |
|---|---|---|
| 6.0 | 6.1.0.7 への移行が必要 | 6.1.0.7 への移行が必要 |
| 6.0.1 | 6.1.0.7 への移行が必要 | 6.1.0.7 への移行が必要 |
| 6.1.0 | 6.1.0.7 | 6.1.0.7 |
| 6.2.0 | 6.2.0.7（リリース予定） | 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 | 6.2.2.5（リリース予定） | 6.2.2.5（リリース予定） |
| 6.2.3 | 6.2.3.4 | 6.2.3.4 |

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-asa-dma-dos

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | Date |
|---|---|---|---|---|
| 1.1 | 諮問テキストを一致する更新済諮問メタデータ。 | | 最終版 | 2018-October-29 |
| 1.0 | 初回公開リリース | | 最終版 | 2018 年 10 月 3 日 |

## 利用規約