Cisco FirePOWER の検出エンジンの SSL 復号時のメモリ使用による Denial of Service（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20171004-ftd

初公開日 : 2017-10-04 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 : CSCve02069

CVE-2017-12245

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 SSL トラフィックの復号に脆弱性があり、認証されていないリモートの攻撃者により、システム メモリが使い果たされる可能性があります。 このメモリ リークが一定時間継続する場合、デバイスを介したトラフィックの転送が停止するため、Denial of Service（DoS）の状態に発展する可能性があります。

本脆弱性は、Firepower の Snort 検出エンジンによる SSL トラフィックの復号方法と適応型セキュリティ アプライアンス（ASA）ハンドラーとの通知送受信のエラーに起因するものです。 攻撃者が、デバイスを介して、悪意のあるセキュア ソケット レイヤ（SSL）のトラフィックを連続的に送信することにより、この脆弱性を悪用する可能性があります。 このエクスプロイトにより、デバイスがシステム メモリの少ない状態で動作している場合に、攻撃者が DoS の状態を生じさせ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-20171004-ftd

該当製品

脆弱性のある製品

この脆弱性は、Cisco Firepower Threat Defense（FTD）ソフトウェア リリース 6.0.1 以降で、ソフトウェアが次のセクションで説明する状態に設定された上で、次のいずれかのシスコ製品で実行されている場合に影響を及ぼします。

- 次世代ファイアウォール製品群を使用する適応型セキュリティ アプライアンス（ASA）5500-X シリーズ
- 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 シリーズ セキュリティ アプライアンス

影響を受けたデバイスは復号化の 1つ以上の SSL インスペクション ポリシーのために設定され、または既知キー辞職するとき脆弱です。 これらの機能では、さらなる検査のためにデバイスでの SSL トラフィックの復号が許可されます。

本脆弱性は、FTD をサポートするリリースのみに影響します。 これらのリリースには、Firepower のコードと ASA のコードの両方が含まれています。 その他の情報のための Cisco Firepower 互換性 ガイドの確認 Firepower Threat Defense デバイス。

管理者は FTD リリースを判別するのに CLI コマンド **show version** を使用できます。 次の例では、デバイスでソフトウェア リリース 6.2.0 が実行されています。

```
> 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

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

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）
- FirePOWER サービスを使用する適応型セキュリティ アプライアンス（ASA）5000-X シリーズ
- FirePOWER サービスを使用する適応型セキュリティ アプライアンス（ASA）5500-X シリーズ
- ネットワーク向け Advanced Malware Protection（AMP）7000 シリーズ アプライアンス
- ネットワーク向け Advanced Malware Protection（AMP）8000 シリーズ 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 Management Center
- サービス統合型ルータ（ISR）向け FirePOWER Threat Defense
- 侵入防御システム（IPS）ソフトウェア

- VMware 向け仮想次世代侵入防御システム（NGIPSv）

詳細

Cisco FTD は、ASA の機能と Firepower のサービスを含んだ統合ソフトウェア イメージです。この統合ソフトウェアにより、ASA と Firepower の機能を、ハードウェア機能とソフトウェア機能の両面で、単一のプラットフォーム上で提供することが可能となります。

セキュリティ侵害の痕跡

脆弱なデバイスは、次の条件に一致する場合に侵害されます。

- デバイスがトラフィックの転送を止めている。
- **show blocks コマンド**の出力は特定のメモリブロックのゼロ カウントを示したものです。 最も一般的なメモリ ブロックのサイズは、2048 か 9344 です。

```
firepower# show blocks
  SIZE    MAX    LOW    CNT
0 1450 1448 1450 4 100 99 99
80 1000 950 984 256 4148 3898 4040 1550 6279 6184 6258 2048    15864           0
0
  2560    164    164    164
  4096    100    100    100
  8192    100    100    100
  9344    100    100    100
 16384    102    102    102
 65536     16     16     16
```

- debug コマンドの出力は**非対称多重処理システムが**— 100%で… Inspect **dp snort キュー詳細デバッグ**受信キュー 利用を— RxQ （util）示すことを**示します。**

```
firepower# show asp inspect-dp snort queues detail debug
SNORT Inspect Instance Queue Configuration

RxQ-Size:              1   MB
TxQ-Size: 128 KB
TxQ-Data-Limit: 102.4 KB (80%)
TxQ-Data-Hi-Thresh: 35.8 KB (28%) Id QId RxQ RxQ RxQ RxQ TxQ TxQ TxQ TxQ
(used) (util) (max used) (state) (used) (util) (max used) (state) -- ---- ---------- ------
---------- ---------------- ---------- ------ ---------- -------- 0 [0] 2 MB 100%     2   MB
READY              0        0%       2.1 KB   READY
```

- debug コマンドの出力は**非対称多重処理システムが Inspect dp snort カウンター デバッグ ゼロ** ゼロではない受信キューのためのカウントを十分に示すことを**示します**（RxQ 完全な）。

```
 firepower# show asp inspect-dp snort counters debug zeros
SNORT Inspect Instance CountersId   QId  Type  Name                              Value
Raw-Value
-- ---- ---- ---- ---------- ----------
...
All All drop RxQ-Full 146.5 K (146546)
All All drop TxQ-Full 0 (0)
```

この脆弱性の不正利用によりデバイスが侵害されていないか確認する上で支援が必要な場合は、Cisco Technical Assistance Center（TAC）までご連絡ください。

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 TAC もしくは契約しているメンテナンス プロバイダーまで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

カスタマーは、このセクションの表に沿って、適切なリリースへのアップグレードをおこなってください。 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-20171004-fpsnort: Cisco FirePOWER の検出エンジンにおける IPv6 Denial of Service（DoS）の脆弱性

- cisco-sa-20171004-ftd: Cisco FirePOWER の検出エンジンの SSL 復号時のメモリ使用による Denial of Service（DoS）の脆弱性

次の表では、左の列にシスコ ソフトウェアのメジャー リリースを示します。 中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。 右の列が示すのは、一連のアドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、およびそれらの脆弱性に対する最新の推奨リリースです。

Cisco Firepower Threat Defense ソフトウェア	この脆弱性に対する最初の修正リリース	この脆弱および一連のアドバイザリに記載さ
6.0 以前	非サポート	N/A
6.0.1	脆弱性あり; 6.2.0.2 への移行が必要	6.2.0.2
6.1.0	6.1.0.6（リリース予定）	6.1.0.6（リリース予定）、または 6.2.0.2
6.2.0	6.2.0.2 以降	6.2.0.3
6.2.1	脆弱性あり; 6.2.2 への移行が必要	6.2.2
6.2.2	6.2.2	6.2.2

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 TAC のサポート案件の対応時に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-ftd

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017 年 10 月 4 日

利用規約

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。