Cisco FirePOWER の検出エンジンにおける IPv6 Denial of Service（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20171004-fpsnort

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 : CSCvd34776

CVE-2017-12244

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 システム ソフトウェアには、IPv6 パケットの解析を行う検出エンジンに脆弱性があります。認証されていないリモートの攻撃者によって Snort のプロセスの予期せぬ再起動が行われ、CPU が大量に消費されたり、Denial of Service（DoS）状態に陥ったりする可能性があります。

本脆弱性は、IPv6 拡張ヘッダー パケットのフィールドに対する不適切な入力検証に起因します。攻撃者が、標的となったデバイスの検出エンジンに不正な IPv6 パケットを送信することにより、この脆弱性を不正利用する可能性があります。 このエクスプロイトにより、Snort プロセスが再起動され、トラフィック検査がバイパスされるかトラフィックがドロップされた場合、攻撃者が DoS の状況を生じさせる可能性があります。 本脆弱性は、IPv6 トラフィックの場合にのみ影響が及びます。

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-fpsnort

該当製品

脆弱性のある製品

この脆弱性は、Cisco FirePOWER システム ソフトウェア リリース 6.0 以降で、1 つ以上のフ

ァイル アクション ポリシーが設定され、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。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISR）
- 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
- 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
- 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
- サービス統合型ルータ（ISR）向け FirePOWER Threat Defense
- 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
- VMware 向け仮想次世代侵入防御システム（NGIPSv）

Cisco FirePOWER システム ソフトウェアで何らかのファイル アクション ポリシーが設定されているかを確認するには、管理者は FirePOWER システムのダッシュボードで次の操作を実行します。

1. **> アクセスコントロール > Malware およびファイル** 『Policies』 を選択 して下さい。 システムに設定されたファイル アクション ポリシーのリストがダッシュボードに表示されます。
2. ポリシーについては現在の保存された 設定についての詳細を参照するためにポリシーの隣で **Report アイコンを**クリックして下さい。

各ファイルのアクション ポリシーで、特定の基準を満たすファイルの処理方法を定義する規則とアクションのセットを指定します。 1つ以上のポリシーが**ブロック ファイルを**規定 するか、**Malware をブロックするか**、または**ファイル**操作を**検出する**、システムは脆弱です。

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、Cisco FirePOWER システム ソフトウェア リリース 5.3、5.4.0、5.4.1 では本脆弱性の影響が及ばないことを確認しています。

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。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Management Center
- 侵入防御システム（IPS）ソフトウェア
- Meraki MX セキュリティ アプライアンス

- サービス統合型ルータ（ISR）向け Snort IPS
- Sourcefire 3D システム アプライアンス

詳細

この脆弱性により、Snort のプロセスが再起動させられる可能性があります。 Snort のプロセスが再起動している間には、Snort による検出がバイパスされる、もしくはすべてのネットワークトラフィックの検査に失敗する可能性があります。 この動作は、プラットフォームと設定により異なります。

Firepower プラットフォーム

FirePOWER プラットフォームでは、次のような動作が発生します。

- パッシブ インターフェイスおよびバイパス インターフェイスでは、Snort による検査がバイパスされ、トラフィックがデバイスを通過します。
- ルーティング インターフェイス、スイッチング インターフェイス、非バイパス インターフェイスでは、トラフィックがドロップされ、デバイスを通過しません。
- Firepower Threat Defense（TFD）では、トラフィックがドロップされ、デバイスを通過しません。

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

ASA リリースが故障する**開いた** CLI コマンド **sfr を**サポートし、このコマンドが設定されれば、トラフィックは Snort をバイパスし、廃棄されません。

セキュリティ侵害の痕跡

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 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

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 システム 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	脆弱性なし	N/A

6.0.1	6.0.1.4 (リリース予定)	6.2.0.2
6.1.0	6.1.0.3	6.1.0.6 (リリース予定) 、または 6.2.0.2
6.2.0	6.2.0.2	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	脆弱性なし	6.2.2

FirePOWER システム ソフトウェアをアップグレードするには、次の方法のいずれかを使用します。

- Firepower Management Center (FMC) を使用してソフトウェアをアップグレードする場合は、修正済みリリースのソフトウェアをインストールし、インストール後にアクセス制御ポリシーを再度適用してください。 インストールされる Snort のバージョンは、FMC のソフトウェア リリースにより異なります。
- Adaptive Security Device Manager (ASDM) 、もしくは Firepower Device Manager (FDM) を使用してソフトウェアをアップグレードする場合は、修正済みリリースのソフトウェアへアップグレードし、インストール後にアクセス制御ポリシーを再度適用してください。

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

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-fpsnort

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

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。