Cisco Firepower Threat Defenseソフトウェアの TCP Snort 3検出エンジンバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snort-bypass-PTry37fX
CVE-2024-20407
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwi42291

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TCPインターセプト機能とSnort 3検出エンジン間のインタラクションにおける脆弱性により、認証されていないリモートの攻撃者が、該当システムで設定されたポリシーをバイパスできる可能性があります。Snort 2が設定されたデバイスは、この脆弱性の影響を受けません。

この脆弱性は、初期（ハーフオープン）TCP接続を処理する際の論理エラーが原因です。攻撃者は、該当デバイスを介して巧妙に細工されたトラフィックパターン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。不正利用に成功すると、意図しないトラフィックが該当デバイスによって保護されているネットワークに侵入され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ています。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-bypass-PTry37fX

このアドバイザリは、2024年10月に公開されたCisco ASA、FMC、およびFTDソフトウェアセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月』を参照してください。

該当製品

脆弱性のある製品

公開時点で、Cisco FTDソフトウェアおよびCisco FirePOWERサービスが、Snort 3検出エンジンを使用して最大初期接続を使用して設定されている場合、この脆弱性の影響を受けました。

脆弱性が存在する Cisco ソフトウェア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 FTDソフトウェアでのSnort設定の確認

Snort 3がCisco FTDソフトウェアで実行されているかどうかを判別するには、「Firepower Threat Defense(FTD)で実行されているアクティブなSnortバージョンの判別」を参照してください。この脆弱性を不正利用するには、Snort 3がアクティブである必要があります。

Cisco FTDソフトウェアの初期構成の確認

初期接続のデフォルト値は0で、接続に制限はありません。デフォルト設定を使用した導入には脆弱性は存在しないと考えられます。

初期接続設定を確認するには、show running-config policy-map | include embryonic FTD CLIコマンドを使用します。次の例は、最大初期接続が設定されているデバイスでのコマンドの出力を示しています。

```
<#root>

FTD#

show running-config policy-map | include embryonic


  set connection conn-max 1000 embryonic-conn-max 3000
FTD#
```

コマンドの出力に何も表示されない場合、そのデバイスは脆弱性が存在しないと見なされます。

初期接続の詳細については、『Cisco Secure Firewall Management Centerデバイスコンフィギュレーションガイド』の「SYNフラッドDoS攻撃（TCPインターセプト）からのサーバの保護」セクションまたは「接続設定について」セクションを参照してください。

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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Cisco Secure Firewall Management Center(FMC)ソフトウェア（旧称：Firepower Management Center Software）
- オープンソースの Snort 2
- オープンソースの Snort 3

回避策

この脆弱性に対処する回避策はありません。この回避策を実装するには、次の例に示すように、FTD CLIコマンドのno asp inspect-dp pkt-decode-optimizationを使用して、pkt-decode-optimizationをオフにします。

```
<#root>

FTD#

no asp inspect-dp pkt-decode-optimization

FTD#
```

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスクを判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソ

フトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

Cisco FTDデバイスのアップグレード手順については、該当する『Cisco FMC upgrade guide』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている

脆弱性の不正利用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 サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-bypass-PTry37fX

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2024年10月23日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。