Snort検出エンジンによるCisco Firepower Threat Defenseソフトウェアの脆弱性データベースにおけるセキュリティポリシーバイパスとサービス妨害(DoS)の問題

アドバイザリーID : cisco-sa-ftd-vdb-snort-djj4cnbR
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
回避策 : No workarounds available
Cisco バグ ID : CSCwm79091

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Cisco Vulnerability Database(VDB)リリースに関する問題により、トラフィックを検査するときにSnort検出エンジンが予期せず再起動する可能性があります。Snort検出エンジンの再起動中に、デバイスの設定に応じて、トラフィックがSnortインスペクションをバイパスしたり、ドロップされたりする可能性があります。詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

Snort 2およびSnort 3検出エンジンはどちらも影響を受けます。Snort検出エンジンが自動的に再起動します。手動による介入は必要ありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-vdb-snort-djj4cnbR

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。

脆弱性のある製品

この問題は、Cisco VDBリリース396を実行しているCisco FTDソフトウェアに影響します。

Cisco VDBリリースの確認

Cisco FTDデバイスで実行されているCisco VDBリリースを確認するには、次の例に示すように、show version CLIコマンドを使用します。

```
<#root>

FTD>

show version


-------------[ ftd-fmc2-mgmt ]---------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.2.8 (Build 25)
UUID                      : a0ed2102-6a3e-11ef-b9a6-b8830d51972b
LSP version               : lsp-rel-20240930-1858
VDB version               :

396


-----------------------------------------------------
FTD>
```

VDB version行を表示します。リリースが396の場合、このアドバイザリで説明されている問題が存在します。これ以外のリリースがリストされている場合は、このアドバイザリに記載されている問題はありません。

Cisco Secure Firewall Management Center(FMC)ソフトウェア（旧Firepower Management Center、GUI）のCisco VDBのリリースを表示するには、Help > Aboutの順に選択します。

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リストされている製品だけがこの問題の影響を受けることが知られています。

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 FMC ソフトウェア
- オープンソースの Snort 2
- オープンソースの Snort 3

詳細

Snortプロセスが再起動した場合のトラフィックの処理方法は、次のCisco FTDソフトウェアSnort検出エンジンの設定パラメータによって決まります。

- Snortのフェールオープン
- snort preserve-connection（接続保存）

詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「Snortリスタートトラフィック動作」セクション、または『Cisco Defense Orchestrator』ガイドの「Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center」を参照してください。

回避策

この問題に対処する回避策はありません。

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。

修正済みリリース

このドキュメントの発行時点で、Cisco VDBリリース397以降を実行しているCisco FTDソフトウェアには、この問題に対する修正が含まれています。Cisco VDBリリース396は、Cisco Software Download Centerから削除されました。

最新情報については、アドバイザリ上部のバグIDの「詳細」セクションを参照してください。

Cisco VDBのアップグレードの詳細については、次のリソースを参照してください。

- 『Firepower Management Centerコンフィギュレーションガイド』の「脆弱性データベース(VDB)の更新」セクション
- 『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Updating System Databases」セクション

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRTでは、本アドバイザリに記載されている問題の不正利用事例とその公表は確認して

おりません。

出典

この問題は、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-ftd-vdb-snort-djj4cnbR

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。