複数のシスコ製品におけるSnortレートフィルタバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snort-rf-bypass-OY8f3pnM
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 : No workarounds available
Cisco バグ ID : CSCwf52284 CSCwf93293

CVE-2024-20342

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

Snort検出エンジンのレートフィルタリング機能の脆弱性により、認証されていないリモートの攻撃者が、設定されているレート制限フィルタをバイパスする可能性がある、複数のシスコ製品が影響を受けます。

この脆弱性は、接続カウントの比較が正しく行われないことに起因しています。攻撃者は、設定されたレートフィルタを超えるレートで該当デバイスを介してトラフィックを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はレートフィルタをバイパスできる可能性があります。これにより、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入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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-rf-bypass-OY8f3pnM

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

公開時点では、この脆弱性はOpen Source Snort 2およびOpen Source Snort 3に影響を与えました。

公開時点では、この脆弱性は、Cisco FirePOWER ServicesまたはCisco Firepower Threat Defense(FTD)ソフトウェアの脆弱性が存在するリリースを実行していて、Snortが有効になっているシスコ製品にも影響を与えました。

公開時点で脆弱性が確認されている Cisco 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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。
Snortの詳細については、Snort Webサイト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
- Cyber Vision ソフトウェア
- Meraki 製品
- Secure Firewall Management Center(FMC)ソフトウェア（旧称：Firepower Management Center Software）
- Unified Threat Defense(UTD)ソフトウェア

詳細

この脆弱性が不正利用されると、攻撃者は該当デバイスに適用されるレートフィルタによる保護をバイパスできる可能性があります。この脆弱性の全体的な影響は、レートフィルタが保護する資産の重要性に依存するため、組織によって異なります。お客様は、この脆弱性の不正利用がネットワークに与える影響を評価し、お客様独自の脆弱性処理および修復プロセスに従って作業を進める必要があります。

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

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は、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列にはソフトウェアリリースが、右の列には、そのリリースが本アドバイザリに記載された脆弱性の影響を受けたかどうか、また本アドバイザリに対する修正を含むリリースが示されています。

Cisco FTD ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
7.0 以前	7.0.6.2
7.1	修正済みリリースに移行。
7.2	7.2.6
7.3	修正済みリリースに移行。
7.4	7.4.2.1
7.6	脆弱性なし

注：Snort 2は修正されず、上記の表に記載されている修正済みリリースではSnort 3を有効にする必要があります。Cisco FMCを使用してSnort 3を有効にするには、『Firepower Management Center Snort 3コンフィギュレーションガイド』を参照してください。Cisco Firepower Device Manager(FDM)を使用してスタンドアロンデバイスでSnort 3を有効にするには、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Snort 2とSnort 3の切り替え」を参照してください。

オープンソースSnortリリース	First Fixed Release（修正された最初のリリース）
Snort 2	Snort 3に移行。
Snort 3	3.1.74.0

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脆弱性の不正利用事例やその公表は確認しておりません。

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-rf-bypass-OY8f3pnM

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。