CiscoFirepower脅威対策ソフトウェアのSnort 3位置情報IPフィルタバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-ftdsnort3sip-bypass-LMz2ThKn
初公開日 : 2023-11-01 16:00
バージョン 1.0 : Final
CVSSスコア : 4.0
回避策 : Yes
Cisco バグ ID : CSCwe69833

CVE-2023-20267

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 3のIP位置情報ルールの脆弱性により、認証されていないリモートの攻撃者がIPアドレス制限をバイパスできる可能性があります。

この脆弱性は、IP位置情報ルールの設定が適切に解析されないことに起因しています。攻撃者は、制限をバイパスするまでIPアドレスをスプーフィングすることで、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、攻撃者はロケーションベースのIPアドレス制限をバイパスでき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-ftdsnort3sip-bypass-LMz2ThKn

このアドバイザリは、Cisco ASA、FTD、およびFMCセキュリティアドバイザリバンドル公開の2023年11月版リリースの一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: November 2023 Semiannual Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication』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Cisco FTDソフトウェアが脆弱なリリースを実行していて、Snort

3検出エンジンが地理位置情報インスペクションポリシーで設定されている場合に影響を受けました。

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確認するには、「Firepower脅威対策(FTD)で実行されるアクティブな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をアクティブにする必要があります。

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 Firepower Management Center（FMC）ソフトウェア
- オープンソースSnort 2
- オープンソースSnort 3

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ACLによって提供され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、ACL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、自身の脆弱性処理および修復プロセスに従って処理を進める必要があります。

セキュリティ侵害の痕跡

『Cisco Security Indicators of Compromise Reference Guide』にはよく見られる IoC が記載されており、このシスコ セキュリティ アドバイザリで公開されている脆弱性の影響を受ける可能性のあるデバイスを特定するのに役立ちます。

回避策

この脆弱性に対処する回避策はありません。

位置情報コンフィギュレーションファイルで、最後のエントリとして重大ではないIP除外範囲を設定します。このエントリは無視されます。

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

FTD デバイスのアップグレード手順については、Cisco Firepower Management Center アップグレードガイドを参照してください。

関連情報

最適な Cisco ASA、FTD、または FMC 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-ftdsnort3sip-bypass-LMz2ThKn

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	2023年11月1日

利用規約

する権利を有します。
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。

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。