複数のシスコ製品におけるSnort 3 HTTP侵入防御システム(IPS)ルールバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snort3-ips-bypass-uE69KBMd
CVE-2024-20363
初公開日 : 2024-05-22 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 : CSCwh73244 CSCwh22565

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侵入防御システム(IPS)ルールエンジンの脆弱性により、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ているルールをバイパスする可能性のある、複数のシスコ製品が影響を受けます。

この脆弱性は、不適切なHTTPパケット処理に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたHTTP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。エクスプロイトに成功すると、攻撃者は設定されたIPSルールをバイパスし、ネットワーク上の検査されていないトラフィックを許可す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-snort3-ips-bypass-uE69KBMd

このアドバイザリは、2024 年 5 月に公開された Cisco ASA、FMC、および FTD ソフトウェアのセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、『Cisco Event Response: May 2024 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

公開時点でこの脆弱性の影響を受けていた製品については、次のセクションを参照してください。

オープンソースの Snort 3

公開時点で、この脆弱性はオープンソースのSnort 3に影響を与えました。

公開時点で脆弱性が存在していたSnort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。Snortの詳細については、Snort Webサイトを参照してください。

Cisco FirePOWERおよびFirepower Threat Defenseソフトウェア

公開時点では、この脆弱性は、Cisco FirePOWER 4200シリーズファイアウォール用のCisco FirePOWER ServicesおよびCisco Firepower Threat Defense(FTD)ソフトウェアでSnort 3が実行されている場合に、これらに影響を与えました。

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

Cisco FTDソフトウェアリリース7.0.0以降の新規インストールでは、Snort 3がデフォルトで実行されます。Cisco FTDソフトウェアリリース6.7.0以前を実行していて、リリース7.0.0以降にアップグレードされたデバイスでは、デフォルトでSnort 2が実行されます。

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 IOS XE ソフトウェア

公開時点では、Cisco IOS XEソフトウェア用のUnified Threat Defense(UTD)Snort IPS EngineまたはCisco IOS XE SD-WANソフトウェア用のUTD Engineの脆弱性のあるリリースを実行する次のシスコ製品がこの脆弱性の影響を受けました。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ ISR
- Catalyst 8000V エッジソフトウェア
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Catalyst 8500L エッジプラットフォーム
- クラウドサービスルータ 1000V
- サービス統合型仮想ルータ（ISRv）

注：UTDはデフォルトではこれらのデバイスにインストールされていません。UTDファイルがインストールされていない場合、そのデバイスは脆弱ではありません。

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。

UTD が有効かどうかを確認する方法

デバイスでUTDが有効になっているかどうかを確認するには、show utd engine standard statusコマンドを使用します。出力のRunningの下にYesと表示されている場合、UTDはイネーブルです。出力されない場合、デバイスは影響を受けません。次の例は、UTDが有効になっているデバイスでの出力を示しています。

<#root>

```
Router#
show utd engine standard status

Engine version       : 1.0.19_SV2.9.16.1_XE17.3
Profile              : Cloud-Low
System memory        :
             Usage  : 6.00 %
             Status : Green
Number of engines    : 1
```

<#root>

```
Engine
Running

    Health     Reason
=========================================
Engine(#1):
Yes

        Green      None
=========================================================
.
.
.
```

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、この脆弱性がオープンソースのSnort 2には影響を与えないことを確認しました。

また、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
- Firepower Management Center（FMC）ソフトウェア
- Merakiアプライアンス
- Umbrellaセキュアインターネットゲートウェイ(SIG)

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

修正済みリリースの詳細については、次のセクションを参照してください。

オープンソースSnortソフトウェア

発行時点では、次の表に示すリリース情報は正確でした。

Snortリリース	First Fixed Release（修正された最初のリリース）
2.x	脆弱性なし
3.x	3.1.69.0

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	オン	

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

UTD

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。

Cisco IOS XE 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）
17.12 より前	脆弱性なし
17.12	17.12.3
17.13	17.13.1

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-ips-bypass-uE69KBMd

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 5 月 22 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり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。