複数のシスコ製品におけるSnort FTPインスペクションバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snort-ftd-zXYtnjOM
初公開日 : 2023-11-01 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 : CSCwe02137 CSCwd83613 CSCwb69096 CSCwe57521 CSCwd09631

CVE-2023-20071

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に設定されたポリシーをバイパスでき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、Snort検出エンジンのFTPモジュールの欠陥に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたFTPトラフィック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、攻撃者はFTPインスペクションをバイパスし、悪意のあるペイロードを配信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。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-ftd-zXYtnjOM

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

公開時点で脆弱性が存在し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Snortへの影響

公開時点では、この脆弱性はオープンソースのSnort 2とオープンソースのSnort 3に影響を与えました。

脆弱性が存在する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。

シスコのFirepowerサービスおよびFirepower脅威対策製品への影響

公開時点では、この脆弱性は、シスコソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- Firepowerサービス – すべてのプラットフォーム
- Firepower Threat Defense（FTD）ソフトウェア - すべてのプラットフォーム

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 IOS XE製品への影響

公開時点で、Cisco IOS XEソフトウェア用のCisco Unified Threat Defense(UTD)Snort Intrusion Prevention System(IPS)エンジン、またはCisco IOS XE SD-WANソフトウェア用のCisco UTDエンジンの最初の修正済みリリースより前のリリースを実行していた次のシスコ製品が、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 サービス統合型ルータ（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シリーズエッジプラットフォーム
- Cloud Services Router 1000V シリーズ
- 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。

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。

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 コマンドを発行して Running が Yes になっていることを確認します。出力がない場合、デバイスは影響を受けません。次の出力例は、UTDが有効になっているデバイスを示しています。

```
<#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
=============================================================

.
.
.
```

Cisco Meraki製品への影響

公開時点では、この脆弱性は、シスコソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- Meraki MX64およびMX64Wアプライアンス
- Meraki MX65およびMX65Wアプライアンス
- Meraki MX67、MX67C、およびMX67Wアプライアンス
- Meraki MX68、MX68W、およびMX68WCアプライアンス
- Meraki MX75アプライアンス

- Meraki MX84アプライアンス
- Meraki MX85アプライアンス
- Meraki MX95アプライアンス
- Meraki MX100アプライアンス
- Meraki MX105アプライアンス
- Meraki MX250アプライアンス
- Meraki MX400アプライアンス
- Meraki MX450アプライアンス
- Meraki MX600アプライアンス

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。

他のシスコ製品への影響

公開時点では、この脆弱性は、シスコソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- Cyber Vision
- Umbrellaセキュアインターネットゲートウェイ(SIG)

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。

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
- Catalyst 8500 シリーズ エッジ プラットフォーム
- Firepower Management Center（FMC）ソフトウェア
- Meraki vMX
- Meraki Z1アプライアンス
- Meraki Z3シリーズアプライアンス

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

公開時点で脆弱性が存在していたSnortおよびシスコソフトウェアリリースについては、次のセクションを参照してください。

CiscoFirepowerおよびFTDソフトウェア

Cisco Software Checkerは、Snort 2とSnort 3で設定されたCisco FTDデバイスを区別しません。設定に依存する修正済み情報および脆弱性のある情報については、次の表を参照してください。設定に依存しない修正済み情報と脆弱性のある情報については、Cisco Software Checkerを参照してください。

設定に依存する情報

次の表では、左の列にシスコソフトウェアのリリースを記載しています。中央の列は、Snort 2用に設定されているCisco FTDソフトウェアリリースが、このアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびその脆弱性に対する修正を含む最初のリリースを示しています。右の列は、Snort 3用に設定されているCisco FTDソフトウェアリリースが、このアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびその脆弱性に対する修正を含む最初のリリースを示しています。

このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco FTD ソフトウェア リリース	CSCwd83613	CSCwb69096
6.3 以前	修正済みリリースに移行。	影響なし。
6.4	6.4.0.17	影響なし。
6.5	修正済みリリースに移行。	影響なし。
6.6	修正済みリリースに移行。	影響なし。

Cisco FTD ソフトウェア リリース	CSCwd83613	CSCwb69096
6.7	修正済みリリースに移行。	修正済みリリースに移行します。[1]
7.0	7.0.6	7.0.5
7.1	修正済みリリースに移行。	7.1.0.3
7.2	7.2.4	7.2.1
7.3	7.3.1.2（2024年3月）	脆弱性なし

1. Snort 3の設定オプションは、Cisco FTDリリース6.7でCisco FDMによって管理されるデバイスでのみ使用できます。

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

その他のプラットフォーム

発行時点では、次の表に記載されているリリース情報は正確でした。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

サイバービジョン：CSCwd09631

Cisco Cyber Visionリリース	First Fixed Release（修正された最初のリリース）
3.2.4 以前	修正済みリリースに移行。
4.0	修正済みリリースに移行。
4.1	4.1.3

UTDソフトウェア：CSCwe57521

Cisco UTD 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）
17.3	17.3.8
17.6	17.6.6
17.9	17.9.4
17.11	17.11.1a
17.12	17.12.1a

Meraki MX セキュリティ アプライアンス

Cisco Meraki MXセキュリティアプライアンスリリース	First Fixed Release（修正された最初のリリース）
MX15以前	修正済みリリースに移行。
MX16	MX 16.6.6以降で利用可能なホットフィックス。
MX17	MX 17.0以降で利用可能なホットフィックス。
MX18	MX 18.1以降でホットフィックスが利用可能です。

注：MX64およびMX65プラットフォームには修正は提供されません。

オープンソースのSnortソフトウェア

Snortリリース	First Fixed Release（修正された最初のリリース）
Snort 2	Snort 3に移行します。
Snort 3	3.1.32.0

包括SIG

シスコは、クラウドベースのCisco Umbrella SIGでこの脆弱性に対処しています。ユーザの対処は必要ありません。

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-snort-ftd-zXYtnjOM

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

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。