複数のシスコ製品のSNORT HTTP検出エンジンのファイルポリシーバイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-ftd-bypass-3eCfd24j **初公開日 :** 2020-10-21 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 :** CSCvq96573 CSCvm69545	CVE-2020-3299

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

複数のシスコ製品は、Snort検出エンジンの脆弱性の影響を受け、認証されていないリモートの攻撃者がHTTP用に設定されたファイルポリシーをバイパスする可能性があります。

この脆弱性は、チャンクされた応答で使用される変更されたHTTPパケットの誤った検出に起因します。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HTTPパケット用に設定されたファイルポリシーをバイパスし、悪意のあるペイロードを配信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ました。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-bypass-3eCfd24j

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、シスコの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。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 4000 シリーズ サービス統合型ルータ（ISR）
- Cloud Services Router 1000V
- Firepower Threat Defense（FTD）ソフトウェア
- Integrated Services Virtual Router(ISRv)
- Meraki MXシリーズセキュリティアプライアンス[1]

1. 例外については、このアドバイザリの「脆弱性が存在しない製品」セクションを参照してください。

この脆弱性は、2.9.13.1より前のオープンソースSnortプロジェクトのバージョンにも影響を与えます。詳細については、Snort Webサイトを参照してください。

公開時点で脆弱性が存在していたシスコ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。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。

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脆弱性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
- Firepower Management Center（FMC）ソフトウェア
- Meraki MX64セキュリティアプライアンス
- Meraki MX64Wセキュリティアプライアンス
- Meraki vMX100仮想アプライアンス
- 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。緩和策については、TACにお問い合わせください。

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完全なアップグレード ソリューション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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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

発行時点では、次の表のリリース情報が正確でした。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。

左側の列にはCiscoソフトウェアリリースがリストされ、右側の列には、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たリリースと、この脆弱性に対する修正が含まれているリリースが示されています。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.01	6.3.0.1
6.0.11	6.3.0.1
6.1.0	6.3.0.1
6.2.0	6.3.0.1
6.2.1	6.3.0.1
6.2.2	6.3.0.1
6.2.3	6.3.0.1
6.3.0	6.3.0.1
6.4.0	脆弱性なし
6.5.0	脆弱性なし
6.6.0	脆弱性なし

1. Cisco FMCおよびFTDソフトウェアリリース6.0.1以前、およびリリース6.2.0および6.2.1は、ソフトウェアメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

IOS XE向けCisco UTD Snort IPS Engineソフトウェア

UTD SNORT IPS Engine IOS XEリリース	この脆弱性に対する最初の修正リリース
16.9	16.9.5
16.12	16.12.2

17.1	脆弱性なし
17.2	脆弱性なし

最も完全で最新の情報については、バグID CSCvq96573の「詳細」セクションを参照してください。

IOS XE SD-WAN向けCisco UTDエンジンソフトウェア

UTDエンジンIOS XE SD-WANリリース	この脆弱性に対する最初の修正リリース
16.10	16.10.3b
16.12	16.12.1d
17.2	脆弱性なし

最も完全で最新の情報については、バグID CSCvq96573の「詳細」セクションを参照してください。

Meraki MXシリーズセキュリティアプライアンス

Meraki MXシリーズセキュリティアプライアンスリリース	この脆弱性に対する最初の修正リリース
MX 14	MX 14.53
MX 15	MX 15.33（ベータ）

オープンソースSNORT

これは、オープンソースのSnortプロジェクトバージョン2.9.13.1以降で修正されています。詳細については、Snort の Web サイトを参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、シスコ内部でセキュリティテストを実施中に、Santosh Krishnamurthy によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-bypass-3eCfd24j

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2020年10月21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。