複数のシスコ製品のSnort HTTP Detection Engine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-snort_filepolbypass-m4X5DgOP **初公開日 :** 2020-05-06 16:00 **最終更新日 :** 2020-05-08 15:54 **バージョン 1.1 :** Final **CVSSスコア :** 5.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvr82603 CSCvt10151 CSCvt28138 CSCvr01675	CVE-2020-3315

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

複数のシスコ製品がSnort検出エンジンの脆弱性の影響を受けます。これにより、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たファイルポリシーをバイパスできる可能性があります。

この脆弱性は、Snort検出エンジンによる特定のHTTP応答の処理方法にエラーが発生することに起因します。攻撃者は、該当システムを通過する巧妙に細工された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ファイルポリシーをバイパスし、保護されたネットワークに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-snort_filepolbypass-m4X5DgOP

該当製品

脆弱性のある製品

公開時点で、この脆弱性は次のシスコ製品で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場合に影響を受けます。

- 1000シリーズサービス統合型ルータ(ISR)[1]
- 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 シリーズ
- Firepower Threat Defense（FTD）ソフトウェア
- Integrated Services Virtual Router(ISRv)[1]

1.この脆弱性の影響を受けるのは、Cisco IOS XE SD-WANソフトウェアイメージを実行している製品のみです。

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。

この脆弱性は、リリース2.9.16より前のすべてのオープンソースSnortプロジェクトに影響を与えました。詳細については、Snortの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 MX セキュリティ 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、Cisco Security Advisories and Alerts 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

Cisco FTD ソフトウェア

公開時点で、Cisco FTDソフトウェアリリース6.6.0以降には、この脆弱性に対する修正が含まれていました。[1]

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。

1. Cisco FMC および FTD ソフトウェア リリース 6.0.1 以前については、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。

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

公開時点では、Cisco IOS XEソフトウェアリリース17.2.1r以降のCisco Unified Threat Defense(UTD)Snort Intrusion Protection System(IPS)Engineソフトウェアに、この脆弱性のCSCvt10151の修正が含まれています。

公開時点で、シスコはCisco IOS XEソフトウェア用のCisco Unified Threat Defense(UTD)Snort Intrusion Protection System(IPS)エンジンソフトウェアに関するこの脆弱性のCSCvt28138部分に対処するアップデートををリリースしていません。

最も完全で最新の情報については、バグID CSCvt10151およびCSCvt28138の「詳細」セクションを参照してください。

Cisco IOS XE SD-WANソフトウェア用Cisco UTD Snort IPS Engineソフトウェア

公開時点では、シスコはCisco IOS XE SD-WANソフトウェア向けCisco UTD Snort IPS Engineソフトウェアに関するこの脆弱性に対処するアップデートをリリースしていません。

最も完全で最新の情報については、バグID CSCvt10151およびCSCvt28138の「詳細」セクショ

ンを参照してください。

オープンソースSnort

公開時点で、オープンソースのSnortプロジェクトのリリース2.9.16以降には、この脆弱性に対する修正が含まれていました。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-snort_filepolbypass-m4X5DgOP

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	Cisco IOS XEソフトウェア用Cisco UTD Snort IPS Engineの修正済みリリース情報を追加。	修正済みリリース	最終版	2020年5月8日
1.0	初回公開リリース	—	最終版	2020 年 5 月 6 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。