複数のシスコ製品のSnort HTTP Detection Engine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-http-fp-bp-KfDdcQhc **初公開日 :** 2021-04-28 16:00 **最終更新日 :** 2021-05-20 18:51 **バージョン 1.1 :** Final **CVSSスコア :** 5.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvw59055 CSCvw19272 CSCvv70864 CSCvw26645	CVE-2021-1494 CVE-2021-1495

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て、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。

これらの脆弱性は、特定のHTTPヘッダーパラメータの不適切な処理に起因します。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、これら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HTTPパケットに対して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。

シスコはこれら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。これら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-http-fp-bp-KfDdcQhc

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はリリース2.9.17.1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。オープンソースSnortの詳細については、SnortのWebサイトを参照してください。

公開時点で、Cisco IOS XEソフトウェア用Cisco UTD Snort IPS Engineソフトウェアまたは Cisco IOS XE SD-WANソフトウェア用Cisco UTD Engineを実行し、Snort HTTP Detection Engineのファイルポリシーが設定されている場合、次のシスコの製品にに脆弱性がが影響されます。

- 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）
- 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
- Firepower Threat Defense（FTD）ソフトウェア
- サービス統合型仮想ルータ（ISRv）
- オープンソースSnort 2

リリース時に脆弱性が存在し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。

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、これら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、これらの脆弱性が次のシスコ製品に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 MX セキュリティアプライアンス
- オープンソースSnort 3

回避策

これら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

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。

左側の列にはシスコソフトウェアリリースが一覧表示され、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、これらの脆弱性に対する修正が含まれているリリースが表示されます。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	これらの脆弱性に対する最初の修正リリース
6.2.21 より前	修正済みリリースに移行。
6.2.2	修正済みリリースに移行。
6.2.3	修正済みリリースに移行。
6.3.0	修正済みリリースに移行。
6.4.0	6.4.0.12
6.5.0	修正済みリリースに移行。
6.6.0	6.6.42
6.7.0	6.7.0.2

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 6.2.0、6.2.1 については、ソフトウェアの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。

2. 6.6.0 コードトレインに関する最初の修正済みリリースは 6.6.3 ですが、CSCvx86231 に関連するアップグレードの問題のため、推奨されるリリースは 6.6.4 です。

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 ソフトウェアおよび Cisco IOS XE SD-WAN ソフトウェア

IOS XE用Cisco UTD Snort IPS EngineソフトウェアおよびIOS XE SD-WANソフトウェア用Cisco UTD Engine [1]	これらの脆弱性に対する最初の修正リリース
16.12 より前	修正済みリリースに移行。
16.12	16.12.5
17.1	修正済みリリースに移行。
17.2	修正済みリリースに移行。
17.3	17.3.3
17.4	17.4.1

[1] リリース17.2.1以降、Cisco IOS XEソフトウェアとCisco IOS XE SD-WANソフトウェアは同じイメージファイルを共有します。

オープンソースの Snort

オープンソースのSnortプロジェクトのリリース2.9.17.1以降には、これらの脆弱性に対する修正が含まれています。オープンソースの Snort の詳細については、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とその公表は確認しておりません。

出典

これらの脆弱性は、シスコのSantosh Krishnamurthyが社内セキュリティテストで発見したものです。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-fp-bp-KfDdcQhc

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	アドバイザリにCVE-2021-1494を追加	—	最終版	2021年5月20日
1.0	初回公開リリース	—	最終版	2021-APR-28

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。