Cisco Firepower Threat Defenseソフトウェアの TCP代行受信バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-tcp-intercept-bypass-xG9M3PbY **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 :** CSCvr53058	CVE-2020-3565

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

Cisco Firepower Threat Defense(FTD)ソフトウェアのTCPインターセプト機能の脆弱性により、認証されていないリモートの攻撃者が、該当システムの設定済みアクセスコントロールポリシー（位置情報を含む）とサービス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、初期接続制限に達するとTCPインターセプトが呼び出され、基になる検出エンジンでパケットが誤って処理される可能性があるためです。攻撃者は、TCPインターセプトが設定されているポリシーに一致する巧妙に細工されたトラフィックストリーム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、攻撃者が不正なポリシーに一致する可能性があります。これにより、トラフィックがドロップされるときに転送される可能性があります。さらに、トラフィックが誤ってドロップされ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-tcp-intercept-bypass-xG9M3PbY

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、TCPインターセプトが設定されている場合、6.4.0.8、6.5.0.4、

および6.6.0よりも前のCisco FTDソフトウェアリリースに影響を与えました。

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。

TCPインターセプトが設定されているかどうかを確認する

Cisco Firepower Management Center(FMC)GUIで、[Access Control] > [Access Control] > [Threat Defense Policy]（ルール用）の順に選択し、**[Connections] > [Maximum Embryonic]**および[Connections Per Client] > [Maximum Embryonic]にの値が設定されているかどうかを確認します。

詳細については、「脅威防御サービスポリシー」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。

シスコでは、この脆弱性が Cisco 適応型セキュリティアプライアンス（ASA）ソフトウェアおよび CiscoFirepower Management Center（FMC）ソフトウェアに影響しないことを確認しています。

詳細

デフォルトでは、Cisco FTDデバイスを通過できる接続数に制限はありません。サーバをサービス拒否(DoS)攻撃から保護するために、管理者はポリシールールを使用して特定のトラフィッククラスに制限を設定できます。具体的には、初期接続（TCPハンドシェイクを完了していない接続）に制限を設定すると、SYNフラッディング攻撃から保護されます。初期接続制限を超えると、TCPインターセプトのコンポーネントがプロキシ接続に関与し、攻撃が抑制されることを確認します。

詳細については、「SYNフラッドDoS攻撃（TCPインターセプト）からサーバーを保護する」を参照してください。

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

公開時点では、Cisco FTDソフトウェアリリース6.4.0.8以降、6.5.0.4以降、および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す。

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 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。

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、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcp-intercept-bypass-xG9M3PbY

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 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。