

Cisco Firepower Threat Defense ソフトウェアファイル ポリシー バイパスの脆弱性

Medium	アドバイザリーID : cisco-sa-20190807-ftd-bypass	CVE-2019-1970
m	初公開日 : 2019-08-07 16:00	
	最終更新日 : 2019-08-20 13:28	
	バージョン 1.1 : Final	
	CVSSスコア : 5.8	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvo11350	

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 Secure Sockets Layer (SSL) /Transport 層 セキュリティ (TLS) プロトコル インスペクション エンジンの脆弱性はリモート攻撃者非認証が影響を受けたシステムの設定されたファイル ポリシーをバイパスするようにする可能性があります。

脆弱性は特定の SSL/TLS メッセージを処理するときエラーが原因です。攻撃者は影響を受けたシステムをフローする巧妙に細工された HTTP パケットの送信によってこの脆弱性を不正利用する可能性があります。正常なエクスプロイトは攻撃者が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渡すことを可能に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。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-ftd-bypass>

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco FTD ソフトウェア リリースを先に実行していたリリース 6.4.0 よりシスコ製品に影響を及ぼし、設定されたファイル ポリシーがありました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

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[脆弱性が存在する製品の](#)セクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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

出版物の時に、Cisco FTD ソフトウェアリリース 6.4.0 およびそれ以降はこの脆弱性のための修正が含まれていました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

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

この脆弱性は内部 保全テストの間に Cisco の Santosh Krishnamurthy によって発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-ftd-bypass>

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	更新済ソース情報。	Source	最終版	2019-August-20
1.0	初回公開リリース		最終版	2019年8月7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、単独の転載や意識を施した場合、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。