

Cisco ImmUNET および Cisco AMP for Endpoints システムは脆弱性を Denial of Service (DoS/DDoS) スキャンします

Medium	アドバイザーID : cisco-sa-20181107-imm-dos	CVE-2018-15437
	初公開日 : 2018-11-07 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 5.5	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvk70945	
	CSCvn05551	

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 ImmUNET および Microsoft ウィンドウで動作するエンドポイントのための Cisco Advanced Malware Protection (AMP) のコンポーネントをスキャンするシステムの脆弱性はローカル攻撃者が製品のスキャン機能を無効にすることを可能にする可能性があります。これは実行可能ファイルが脅威のために分析されないでシステムで起動するようにする可能性があります。

脆弱性は不適当なプロセス リソース処理が原因です。攻撃者は Microsoft ウィンドウを稼働するおよび Cisco ImmUNET か Cisco AMP for Endpoints によって保護されたシステムへのローカル アクセスを得ることによっておよび実行する悪意のあるファイルを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可能にする可能性がありますスキャン サービスが防ぎ、最終的にシステムがそれ以上の不正侵入から保護されることを防ぐことを適切に機能することを。

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-20181107-imm-dos>

該当製品

脆弱性のある製品

この脆弱性は Microsoft Windows. で動作する Cisco Immundet および Cisco AMP for Endpoints に影響を与えます 該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID 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

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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。

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

Cisco はこの脆弱性を報告するために ApparitionSec のジョン ページ (hyp3rlinx) に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-imm-dos>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-November-07

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。