

Cisco AMP Threat Grid API 鍵情報公開脆弱性

Medium	アドバイザーID : cisco-sa-20190123-threat-grid	CVE-2019-1657
	初公開日 : 2019-01-23 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 4.3	
	回避策 : No workarounds available	
	Cisco バグ ID :	

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 AMP Threat Grid の脆弱性は機密情報にアクセスする認証される、リモート攻撃者可能にする可能性があります。

脆弱性は API キーの危険な作成が原因です。攻撃者は影響を受けたデバイスに不正アクセスを得るのに不確かな資格情報の使用によってこの脆弱性を不正利用する可能性があります。エクスプロイトは攻撃者が API キー 資格情報の使用によって情報に不正アクセスを得ることを可能にする可能性があります。

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-20190123-threat-grid>

該当製品

脆弱性のある製品

この脆弱性は 3.5.68 前に Cisco AMP Threat Grid Cloud および 2.5 前に Cisco AMP Threat Grid アプライアンス ソフトウェアに影響を与えます。

脆弱性を含んでいないことが確認された製品

このアドバイザーの[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である。

Cisco はこの脆弱性がネットワークのための Cisco AMP に影響を与えないことを確認しました。

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

Cisco AMP Threat Grid Cloud 3.5.68 はクラウドで 2018 年 4月 26 日配置されました。

Cisco AMP Threat Grid アプライアンス ソフトウェア ビルド 2.5 は 2018 年 9月 17 日リリースされました。

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。

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ライアン S.に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-threat-grid>

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	2019-January-23

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。