

Cisco Meeting Server Web Admin インターフェイス Denial of Service (DoS/DDoS) 脆弱性

Medium	アドバイザーID : cisco-sa-20180620-meeting-server-dos	CVE-2018-0371
	初公開日 : 2018-06-20 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.5	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvi48624	

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 Meeting Server の Web Admin インターフェイスの脆弱性はサービス拒否 (DoS) 状態を引き起こす認証される、リモート攻撃者可能にする可能性があります。

脆弱性は着信 HTTP 要求の不十分な確認が原因です。攻撃者は影響を受けた Cisco Meeting Server の Web Admin インターフェイスへ巧妙に細工された HTTP 要求を送信すること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システムを再始動することを可能にし、すべての進行中のコールに影響を受けた製品の DoS 条件に終って終了します。

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-20180620-meeting-server-dos>

該当製品

脆弱性のある製品

この脆弱性は Cisco Meeting Server の次のリリースに該当します:

- Acano X シリーズ
- Cisco Meeting Server 1000

- Cisco Meeting Server 2000

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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#) 他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

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 AXA グループ セキュリティのヒューゴ Boutinon に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-meeting-server-dos>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-June-20

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。