

Cisco Expressway シリーズおよび Cisco TelePresence Video Communication Server (VCS) サービス拒否の脆弱性

Medium	アドバイザーID : cisco-sa-20190417-ces-tvcs-dos	CVE-2019-1720
	初公開日 : 2019-04-17 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.8	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvn99036	

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 Expressway シリーズの XML API および Cisco TelePresence Video Communication Server (VCS) の脆弱性は 100% に影響を受けたシステムのサービス拒否 (DoS) 条件を引き起こす利用により高めるために CPU 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 XML 入力の不適当な処理が原因です。攻撃者はとりわけ巧妙に細工された XML ペイロード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システムが手動でリブートされるまで攻撃者が DoS 状態に終って CPU リソースを、枯渇させ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-20190417-ces-tvcs-dos>

該当製品

脆弱性のある製品

この脆弱性は Cisco Expressway シリーズに Cisco TelePresence Video Communication

Server (VCS) 影響を与え。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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ces-tvcs-dos>

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-April-17

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。