

Cisco TelePresence コラボレーション エンドポイントおよび RoomOS オーディオ盗聴脆弱性

Medium	アドバイザリーID : cisco-sa-20191106-telece-ros-eve	CVE-2019-15967
	初公開日 : 2019-11-06 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 4.4	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvq29891	

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 TelePresence コラボレーション エンドポイント (CE) および Cisco RoomOS ソフトウェアの CLI の脆弱性はユーザに通知しないで録音を有効にする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は不必要な debug コマンドの存在が原因です。 攻撃者は制限シェルにによって得、特定の debug コマンドを使用することこの脆弱性を無制限のアクセス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ユーザに通知しないでオーディオを記録することを影響を受けたデバイスのマイクロフォンが可能にするよう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-20191106-telece-ros-eve>

該当製品

脆弱性のある製品

パブリケーション、この脆弱性の時影響を受けられた Cisco TelePresence CE ソフトウェア リリース リリース 9.8.1 より先におよび Cisco RoomOS ソフトウェア リリース RoomOS 9月 ドロップするより先に 1 2019 年。

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 TelePresence CE ソフトウェア リリース 9.8.1 はおよび Cisco RoomOS ソフトウェア 9月 ドロップするは 1 2019 年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

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

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-November-06

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。