Cisco TelePresence Collaboration EndpointソフトウェアおよびRoomOSソフトウェアのDoS脆弱性

High

アドバイザリーID : cisco-sa-tce-roomos-dos-9V9jrC2q
初公開日 : 2026-02-04 16:00
最終更新日 : 2026-02-12 17:37
バージョン 1.2 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCws04170

CVE-2026-20119

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 Collaboration Endpoint(CE)ソフトウェアおよびCisco RoomOSソフトウェアのテキストレンダリングサブシステムの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、該当デバイスで受信された入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたテキスト（巧妙に細工された会議への招待など）を該当デバイスにレンダリングさせることで、この脆弱性を不正利用する可能性があります。CVSSスコアに示されているように、会議の招待を受け入れるなどのユーザインタラクションは必要ありません。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生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ています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tce-roomos-dos-9V9jrC2q

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco TelePresence CEソフトウェアおよびCisco RoomOSソフトウェアに影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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

シスコは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策（適用可能な場合）を一時的な解決策と見なします。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。中央と右側の列は、リリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

注：リリース10より前のリリースでは、オンプレミスデバイス用のソフトウェアはCisco TelePresence CEソフトウェアと呼ばれ、クラウド導入用のソフトウェアはCisco RoomOSソフトウェアと呼ばれていました。リリース10以降では、オンプレミスとクラウドの両方の導入に対応するソフトウェアをCisco RoomOSソフトウェアと呼びます。Cisco RoomOSソフトウェアのクラウド導入では、標準のリリース番号を使用しません。代わりに、リリース名には、RoomOS 2025年12月など、リリースが利用可能になった月が含まれます。

Cisco TelePresence CEソフトウェアおよびRoomOSソフトウェアリリース	オンプレミス運用における TelePresence CEソフトウェアおよびRoomOSソフトウェアの修正済みリリース	Cloud-Aware運用における RoomOSソフトウェアの修正済みリリース
10 以前	修正済みリリースに移行。	RoomOS 2025年10月版リリース(11.33.1.10) RoomOS 2025年11月版リリース(26.0.1.5)

Cisco TelePresence CEソフトウェアおよびRoomOSソフトウェアリリース	オンプレミス運用における TelePresence CEソフトウェアおよびRoomOSソフトウェアの修正済みリリース	Cloud-Aware運用における RoomOSソフトウェアの修正済みリリース
11	11.27.5.0 11.32.3.0	RoomOS 2025年10月版リリース(11.33.1.10) RoomOS 2025年11月版リリース(26.0.1.5)

シスコの Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tce-roomos-dos-9V9jrC2q

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	修正リリースを更新。	修正済みソフトウェア	Final	2026年2月12日
1.1	修正済みリリースから無関係なテキストを削除。	修正済みリリース	Final	2026年2月10日
1.0	初回公開リリース	—	Final	2026年2月4日

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、単独の転載や意訳を施した場合、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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。