Cisco TelePresenceコラボレーションエンドポイントおよびRoomOSソフトウェアの情報開示の脆弱性

Medium

アドバイザリーID : cisco-sa-roomos-inf-disc-qGgsbxAm
初公開日 : 2025-10-15 16:00
バージョン 1.0 : Final
CVSSスコア : 4.9
回避策 : No workarounds available
Cisco バグ ID : CSCwp08812

CVE-2025-20329

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)およびCisco RoomOSソフトウェアのロギングコンポーネントの脆弱性により、認証されたリモートの攻撃者が該当システムで機密情報をクリアテキストで表示できる可能性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、SIPメディアコンポーネントのロギングが有効な場合に、特定の暗号化されていないクレデンシャルが保存されることに起因します。攻撃者は、該当システムの監査ログにアクセスし、通常はアクセスできないクレデンシャルを取得することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はこれらのクレデンシャルを使用して機密情報にアクセスし、その中には個人を特定できる情報(PII)が含まれていることがあります。

注：Webexクラウドに保存されているログ、またはデバイス自体に保存されているログにアクセスするには、攻撃者が有効な管理者クレデンシャルを持っている必要があります。

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-roomos-inf-disc-qGgsbxAm

該当製品

脆弱性のある製品

この脆弱性の公開時点では、シスコデバイスで次のソフトウェアの脆弱性のあるリリースが実行されており、SIPメディアコンポーネントのロギングが有効にされている場合、これらのデバイスに影響が及びました。

- テレプレゼンスCE
- オンプレミス運用のRoomOS
- クラウドベースのクラウド対応オンプレミス運用のRoomOS

注：ロギングはデフォルトで無効になっています。SIPメディアコンポーネントのロギングは、明示的に設定する必要があります。拡張ロギングを使用している場合は有効になりません。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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

シスコでは、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、回避策や緩和策を検討します。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

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列には、シスコソフトウェアリリースが表示されます。中央と右側の列には、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、およびこれらの脆弱性に対する修正を含むリリースが示されています。

注：リリース9.15以前では、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 July 2025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およびRoomOSリリース	オンプレミス運用における TelePresence CEおよび RoomOSの最初の修正済みリリース	のRoomOSの最初の修正済みリリース クラウド対応の運用
9	修正済みリリースに移行。	修正済みリリースに移行。
10	修正済みリリースに移行。	修正済みリリースに移行。
11	11.32.2.1	RoomOS 2025年7月

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-roomos-inf-disc-qGgsbxAm

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2025年10月15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。