Cisco RoomOS口ギングサブシステムにおける情報開示の脆弱性

Medium

アドバイザリーID : cisco-sa-roomos-infodisc-qBXjfmWm
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 5.7
回避策 : No workarounds available
Cisco バグ ID : CSCwu64817

CVE-2026-20289

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 RoomOSの口ギングサブシステムの脆弱性により、権限の低い認証されたローカル攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、機密情報の口ギングに起因します。攻撃者は、特定の口グレベルを有効にしてシステムログを収集することで、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、攻撃者はユーザログインクレデンシャルなどの機密情報を表示でき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-roomos-infodisc-qBXjfmWm

該当製品

脆弱性のある製品

この脆弱性が公開された時点では、拡張口ギングが有効な場合にCisco RoomOSに影響を与えました。拡張口ギングはデフォルトでは有効になっていません。

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。

拡張ロギングが有効になっているかどうかの確認

拡張ロギングが有効になっているかどうかを確認するには、次の手順を実行します。

1. シスコデバイスの名前またはアドレスを選択します。
   - Board Pro、Desk Mini、Desk Hubを除くすべての製品では、インターフェイスの上部にあります。
   - Board ProとDesk Miniの場合は、右からスワイプしてControl Panelを開きます。
   - Desk Hubの場合、右上隅にあるコントロールアイコンをタップして、コントロールパネルを開きます。
2. デバイスの設定（Board Pro、Desk Mini、またはDesk Hub）または設定（その他の製品）を選択します。
3. Issues and diagnosticsを開き、拡張ロギングトグルボタンのステータスを確認します。

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、回避策や緩和策（該当する場合）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の一時的な解決策であると考えています。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。中央と右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうかを示しています。

Cisco RoomOSリリース	オンプレミス運用でのRoomOSの最初の修正済みリリース	Cloud-Aware運用におけるRoomOSの最初の修正済みリリース
11 以前	今後のリリース	11.39.1.3
26	26.7.2.2	RoomOS 2026年6月(26.7.1.12)

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、クラウド導入用のソフトウェアはCisco RoomOS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はCisco RoomOSと呼ばれます。Cisco RoomOS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、リリースの名前には、リリースが使用可能になった月が含まれます（たとえば、Cisco RoomOSの2023年3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と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-infodisc-qBXjfmWm

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	2026年8月5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。