Cisco RoomOSセキュリティ強化リリース：2026年7月

アドバイザリーID : cisco-sa-hardening-roomos-AqNMbEq
初公開日 : 2026-07-15 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-20150
CVE-2026-20158
CVE-2026-20156
CVE-2026-20157
CVE-2026-20187
CVE-2026-20153

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

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco RoomOSエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、内部で発見された複数の脆弱性に対処するソフトウェア強化リリースが作成されました。

これらの脆弱性はシスコの社内テストで発見されたもので、現在アクティブに悪用されている例は確認されていません。パッチの適用を支援し、開示プロセスを合理化するために、シスコでは、これらの問題を基盤となる脆弱性クラス(Common Weakness Enumeration(CWE))別にグループ化し、各CWEグループにCommon Vulnerabilities and Exposures Identifier(CVE ID)を1つ割り当てました。

シスコはこれら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。これら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-hardening-roomos-AqNMbEq

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco RoomOS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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

次の表に、この強化リリースで対処される脆弱性クラスの概要を示します。各CVE IDに割り当てられるCVSSスコアは、特定のCWEカテゴリ内で最も影響の大きい脆弱性の潜在的な最大重大度を表します。

CVE ID	最高のCVSSスコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-20150	8.8	CWE-284	不適切なアクセス制御（許可、認証、特権、バイパスを含む）
CVE-2026-20153	7.5	CWE-20	不適切な入力検証（入力検証、パストラバーサル、および外部パス制御に対応）
CVE-2026-20156	8.1	CWE-119	メモリバッファの範囲内での操作の不適切な制限（バッファオーバーフローおよび範囲外の書き込みを対象）
CVE-2026-20157	7.5	CWE-311	暗号化の欠落（機密データのクリアテキスト伝送をカバー）
CVE-2026-20158	7.5	CWE-664	リソースのライフタイムを通じた不適切な制御（初期化されていない変数、ヌルポインタ、およびリソースのライフサイクルの問題が対象）
CVE-2026-20187	7.5	CWE-703	例外条件の不適切な処理（捕捉されていない例外と到達可能なアサーションをカバー）

回避策

これら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

これら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。中央および右の列は、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、およびこれらの脆弱性に対する修正を含む最初の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。

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	11.32.6.0	RoomOS 11.39.1.1
26	26.5.2.2	RoomOS 2026年6月(26.7.1.7)

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2026年6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

これらの脆弱性は、既存のテストプロセスとフロンティアAIモデルを使用した内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-roomos-AqNMbEq

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7月15日

利用規約

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。