# Cisco Unified Communications 製品のリモートコード実行の脆弱性


アドバイザリーID : cisco-sa-voice-rce-mORhqY4b
初公開日 : 2026-01-21 16:00
バージョン 1.0 : Final
CVSSスコア : 8.2
回避策 : No workarounds available
Cisco バグ ID : CSCwr29216 CSCwr29208 CSCwr21851

CVE-2026-20045

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 Unified Communications Manager(Unified CM)、Cisco Unified Communications Manager Session Management Edition(Unified CM SME)、Cisco Unified Communications Manager IM & Presence Service(Unified CM IM&P)、Cisco Unity Connection、およびCisco Webex Calling Dedicated Instance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の基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

この脆弱性は、HTTP リクエストでのユーザー入力の検証が不適切なことに起因します。攻撃者は、一連の巧妙に細工されたHTTP要求を該当デバイスのWebベース管理インターフェイスに送信することで、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、基盤となるオペレーティングシステムにユーザレベルでアクセスし、権限をrootに昇格できるようになります。

注：シスコはこのセキュリティアドバイザリのスコアに示されているように、セキュリティ影響評価(SIR)をHighではなくCriticalと設定しています。この脆弱性のエクスプロイトにより、攻撃者が特権をrootに昇格できる可能性があるためです。

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-voice-rce-mORhqY4b

# 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、次のシスコ製品に影響を与えます。

- Unified CM(CSCwr21851)
- Unified CM SME(CSCwr21851)
- Unified CM IM&P(CSCwr29216)
- Unity Connection(CSCwr29208)
- Webex発信専用インスタンス(CSCwr21851)

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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- コンタクトセンターSIPプロキシ
- カスタマーコラボレーションプラットフォーム
- Emergency Responder
- Finesse
- Packaged Contact Center Enterprise（Packaged CCE）
- Prime Collaboration Deployment
- Unified Contact Center Enterprise（Unified CCE）
- Unified Contact Center Express（Unified CCX）
- Cisco Unified Intelligence Center（CUIC）
- Virtualized Voice Browser

# 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のリリースを記載しています。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、およびこ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。

Unified CM、Unified CM IM&P、Unified CM SME、およびWebex発信専用インスタンス

| Cisco Unified CM、Unified CM IM&P、Unified CM SME、およびWebexコール専用インスタンスリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 12.5 | 修正済みリリースに移行。 |
| 14 | 14SU5またはパッチファイルの適用：[1]<br>ciscocm.V14SU4a_CSCwr21851_remote_code_v1.cop.sha512（登録ユーザ専用） |
| 15 | 15SU4（2026年3月）またはapply patch file:[1]<br>ciscocm.V15SU2_CSCwr21851_remote_code_v1.cop.sha512<br>ciscocm.V15SU3_CSCwr21851_remote_code_v1.cop.sha512 |

1. パッチはバージョンによって異なります。詳細については、パッチに添付されているREADMEを参照してください。

Unity Connection

| Cisco Unity Connection リリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 12.5 | 修正済みリリースに移行。 |
| 14 | 14SU5またはパッチファイルの適用：[1]<br>ciscocm.cuc.CSCwr29208_C0266-1.cop.sha512 |
| 15 | 15SU4（2026年3月）またはapply patch file:[1]<br>ciscocm.cuc.CSCwr29208_C0266-1.cop.sha512 |

1. パッチはバージョンによって異なります。詳細については、パッチに添付されているREADMEを参照してください。

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 は、この脆弱性のエクスプロイトが試みられたことを認識しています。この脆弱性が修正済みのソフトウェアリリースにアップグレードすることを強くお勧めします。

## 出典

この脆弱性を報告してくださった外部の研究者に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

## 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1月21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。