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-cucm-rce-bWNzQcUm
初公開日 : 2024-01-24 16:00
最終更新日 : 2024-01-30 19:16
バージョン 1.3 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID : CSCwd64276 CSCwd64245 CSCwe18773 CSCwe18830 CSCwd64292 CSCwe18840

CVE-2024-20253

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

複数の Cisco Unified Communications および Contact Center ソリューション製品の脆弱性により、認証されていないリモートの攻撃者が該当デバイスで任意のコードを実行する可能性があります。

この脆弱性は、メモリに読み込まれるユーザーが提供したデータの不適切な処理に起因します。攻撃者は、該当デバイスのリスニングポートに細工されたメッセージを送信することで、この脆弱性をエクスプロイト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 Web サービスユーザーの権限を使用して、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できる可能性があります。攻撃者は、基盤となるオペレーティングシステムへのアクセス権を使用して、該当デバイスへのルートアクセスを確立することもできます。

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-cucm-rce-bWNzQcUm

該当製品

脆弱性のある製品

この脆弱性は、デフォルト設定の次のシスコ製品に影響を及ぼします。

- Unified Communications Manager（Unified CM）（CSCwd64245）
- Unified Communications Manager IM & プレゼンスサービス（Unified CM IM&P）（CSCwf64276）
- Unified Communications Manager Session Management Edition（Unified CM SME）（CSCwd64245）
- Cisco Unified Contact Center Express（UCCX）（CSCwe18773）
- Unity Connection（CSCwd64292）
- Virtualized Voice Browser（VVB）（CSCwe18840）

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、この脆弱性の影響を受けることが分かっています。

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。

- Customer Collaboration Portal（CCP）（旧 SocialMiner）
- Customer Voice Portal（CVP）
- Emergency Responder（CER）
- Finesse
- Hosted Collaboration Mediation Fulfillment (HCM-F)
- Packaged Contact Center Enterprise（PCCE）
- Prime Collaboration Deployment（PCD）
- Prime License Manager（PLM）
- Remote Expert モバイル
- Unified Contact Center Domain Manager（CCDM）
- Unified Contact Center Enterprise（UCCE）
- Unified Contact Center Management Portal（Unified CCMP）
- Cisco Unified Intelligence Center（CUIC）

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策は使用できます。

Cisco Unified Communications または Cisco Contact Center ソリューションのクラスタをユーザーおよびネットワークの残りの部分から分離する中間デバイスにアクセス制御リスト（ACL）を確立し、展開されたサービスのポートへのアクセスのみ許可します。ポートリストは、使用している音声製品やサービスによって異なります。一部のポートは一時的なポートで、再起動後に変

更されます。

詳細については、『Cisco Unified Communications Manager システム設定ガイド、リリース 14 および SUs』の「Cisco Unified Communications Manager TCP and UDP Port Usage Overview」の項、導入したリリースに対応するバージョン、または最新の シスコ ユニファイド コンタクト センター ソリューションのポート活用ガイド を参照してください。

さらに、最新の『Cisco Unified Communications Manager リリース 14 および SU セキュリティ ガイド』または最新の Cisco Unified ICM/Contact Center Enterprise のセキュリティガイド に記載されているベストプラクティスに従ってください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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 および Unified CM SME：CSCwd64245

Cisco Unified CM および Unified CM SME のリリース	First Fixed Release（修正された最初のリリース）
11.5(1)	修正済みリリースに移行。
12.5(1)	12.5(1)SU8 または ciscocm.v1_java_deserial-CSCwd64245.cop.sha512
14	14SU3 または ciscocm.v1_java_deserial-CSCwd64245.cop.sha512
15	脆弱性なし

Unified CM IM&P：CSCwf64276

Cisco Unified CM IM&P リリース	First Fixed Release（修正された最初のリリース）
11.5(1)	修正済みリリースに移行。
12.5(1)	12.5(1)SU8 または ciscocm.cup-CSCwd64276_JavaDeserialization.cop.sha512
14	14SU3 または ciscocm.cup-

Cisco Unified CM IM&P リリース	First Fixed Release (修正された最初のリリース)
	CSCwd64276_JavaDeserialization.cop.sha512
15	脆弱性なし

Cisco Unity Connection： CSCwd64292

Cisco Unity Connection リリース	First Fixed Release (修正された最初のリリース)
11.5(1)	修正済みリリースに移行。
12.5(1)	12.5(1)SU8 または ciscocm.cuc.v1_java_deserial-CSCwd64292.k4.cop.sha512
14	14SU3 または ciscocm.cuc.v1_java_deserial-CSCwd64292.k4.cop.sha512
15	脆弱性なし

Cisco Unified Contact Center Express： CSCwe18773

Cisco UCCX リリース	First Fixed Release (修正された最初のリリース)
12.0 以前	修正済みリリースに移行。
12.5(1)	ucos.v1_java_deserial-CSCwd64245.cop.sgn[1]
15	脆弱性なし

VVB： CSCwe18840

Cisco VVB リリース	First Fixed Release (修正された最初のリリース)
12.0 以前.	修正済みリリースに移行。
12.5(1)	ucos.v1_java_deserial-CSCwd64245.cop.sgn[1]
12.6(1) および 12.6(2)	ucos.v1_java_deserial-CSCwd64245.cop.sgn[1]
15	脆弱性なし

1. これらの COP ファイルは、特定のリリースにのみ適用されます。これらのリリースのリストと、COP ファイルのインストールに関する追加情報については、COP ファイルに添付されている README ファイルを参照してください。

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された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

シスコは、この脆弱性を報告していただいた Synacktiv 社の Julien Egloff 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	COP ファイルへのリンクを追加。	修正済みリリース	Final	2024 年 1 月 30 日
1.2	緩和策の情報を追加し、修正済みリリースを更新。	「回避策」および「修正済みリリース」	Final	2024 年 1 月 26 日
1.1	影響を受ける製品と脆弱性が存在しないことが確認された製品のリストを更新。	脆弱性のある製品、脆弱性が存在しないことが確認された製品、修正済みリリース	Final	2024 年 1 月 25 日
1.0	初回公開リリース	—	Final	2024 年 1 月 24 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。