複数のCisco Unified Communications製品における認証されていないAPIによる高CPU使用率でのサービス妨害(DoS)の脆弱性

アドバイザリーID : cisco-sa-cucm-apidos-PGsDcdNF
CVE-2023-20259
初公開日 : 2023-10-04 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwf62081 CSCwf62080 CSCwf62074 CSCwf44755 CSCwf62094

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

複数のシスコユニファイドコミュニケーション製品のAPIエンドポイントにおける脆弱性により、認証されていないリモートの攻撃者が高いCPU使用率を引き起こし、Webベースの管理インターフェイスへのアクセスに影響を与え、コール処理の遅延を引き起こす可能性があります。このAPIはデバイス管理には使用されず、デバイスの通常の操作で使用されることはほとんどありません。

この脆弱性は、不適切なAPI認証とAPI要求の不完全な検証に起因します。攻撃者は、巧妙に細工されたHTTP要求をデバイスの特定のAPIに送信することにより、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、CPU使用率が高いためにサービス拒否(DoS)状態が引き起こされ、ユーザトラフィックと管理アクセスに悪影響が及ぶ可能性があります。攻撃が停止すると、デバイスは手動の介入なしで回復します。

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-apidos-PGsDcdNF

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。

- Emergency Responder(CSCwf62074)
- Prime Collaboration導入(CSCwf62080)
- Unified Communications Manager(Unified CM)(CSCwf44755)
- Unified Communications Manager IM & Presence Service(Unified CM IM&P)(CSCwf62094)
- Unified Communications Manager Session Management Edition(Unified CM SME)(CSCwf44755)
- Unity Connection(CSCwf62081)

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。

- Finesse
- Hosted Collaboration Mediation Fulfillment (HCM-F)
- Packaged Contact Center Enterprise（Packaged CCE）
- Prime License Manager（PLM）
- Remote Expert モバイル
- SocialMiner
- Unified Contact Center Domain Manager（Unified CCDM）
- Unified Contact Center Express（Unified CCX）
- Unified Contact Center Management Portal（Unified CCMP）
- Unified Customer Voice Portal（CVP）
- Unified Intelligence Center
- Virtualized Voice Browser(VVB)

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

次の表に示すように、該当する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お勧めします。

Emergency Responder： CSCwf62074

Cisco Emergency Responderリリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
11.5(1) 以前	脆弱性なし	脆弱性なし
12.5(1)	脆弱性なし	脆弱性なし
14	14SU3	ciscocm.cer_V14SU3_CSCwf62074.cop.sha512

Prime Collaboration導入：CSCwf62080

Cisco Prime Collaboration Deploymentリリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
11.5(1) 以前	脆弱性なし	脆弱性なし
12.5(1)	脆弱性なし	脆弱性なし
14	14SU3	ciscocm.V14SU3_pcd_CSCwf62080.k4.cop.sha512

Unified CM UnifiedおよびCM SME: CSCwf44755

Cisco Unified CM および Unified CM SME のリリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
11.5(1) 以前	脆弱性なし	脆弱性なし
12.5(1)	12.5(1)SU7	12.5(1)SU8
14	14SU3	ciscocm.V14SU3_CSCwf44755.cop.sha512

Unified CM IM&P:CSCwf62094

Cisco Unified CM IM&P リリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
11.5(1) 以前	脆弱性なし	脆弱性なし
12.5(1)	12.5(1)SU7	12.5(1)SU8
14	14SU3	ciscocm.cup_CSCwf62094_14SU3.cop.sha512

Unity Connection:CSCwf62081

Cisco Unity Connectionリリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
11.5(1) 以前	脆弱性なし	脆弱性なし
12.5(1)	脆弱性なし	脆弱性なし
14	14SU3	ciscocm.cuc.V14SU3_CSCwf62081.k4.cop.sha512

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

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-cucm-apidos-PGsDcdNF

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	2023年10月4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。