

Cisco Unified Communications Manager セッションの開始プロトコル サービス妨害の脆弱性



アドバイザリーID : [cisco-sa-20190703-cucm-dos](#) [CVE-2019-1887](#)
初公開日 : 2019-07-03 16:00
最終更新日 : 2019-07-08 22:30
バージョン 1.1 : Final
CVSSスコア : [8.6](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvo70834](#)

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 および Unified Communication Manager Session Edition の Session Initiation Protocol (SIP) プロトコル実装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サービス妨害 (DoS) 状態を引き起こす危険性があります。

この脆弱性は、入力 SIP トラフィックの検証が不十分であることに起因しています。攻撃者は、不正な形式の SIP パケットを該当 Cisco Unified Communications Manager または Unified Communications Manager Session Management Edition に送信することにより、この脆弱性をエクスプロイトする可能性があります。攻撃者は、エクスプロイトに成功すると、接続されているすべての電話機で新しい登録プロセスをトリガーし、一時的にサービスを中断させることができるようになります。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucm-dos>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Unified Communications Manager または Unified Communications

Manager Session Management Edition に影響します。

脆弱性が存在する Cisco Unified Communications Manager および Unified Communication Manager Session Management Edition 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。

- Emergency Responder
- Finesse
- Hosted Collaboration Mediation Fulfillment
- MediaSense
- Prime Collaboration Assurance
- Prime Collaboration Provisioning
- Prime License Manager
- SocialMiner
- Unified Communications Manager IM および Presence Service (IM&P)
- Unified Contact Center Express (UCCx)
- Unified Intelligence Center (UIC)
- Unity Connection
- 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。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です。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。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート (Cisco Security Advisories and Alerts)] 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完全なアップグレード ソリューション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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

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、お客様は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か、対応するパッチ ファイルを適用することを推奨します。

Cisco Unified Communications Manager メジャー リリース	修正オプション
10.5(2) 以前	10.5(2) に移行し、パッチ ファイル「 ciscocm.V10-5-2-SU7-SU8 CSCvo70834 C0003-1.cop.sgn 」を適用
10.5(2)	パッチ ファイル「 ciscocm.V10-5-2-SU7-SU8 CSCvo70834 C0003-1.cop.sgn 」を適用
11.5	パッチ ファイル「 ciscocm.V11-5-1-SU5-SU6 CSCvo70834 C0003-1.cop.sgn 」を適用
12.0	パッチ ファイル「 ciscocm.V12-0-1-22900-11 CSCvo70834 C0003-1.cop.sgn 」を適用または 12.0(1)SU3 にアップグレード
12.5	パッチ ファイル「 ciscocm.V12-5-1-10000-22 CSCvo70834 C0003-1.cop.sgn 」を適用または 12.5(1)SU1 にアップグレード

パッチ ファイルは、各リリースのソフトウェア ダウンロード ページの「COP ファイル」セクション Cisco Unity Connection で入手できます。パッチを適用するための手順は、各パッチ ファイルに付属するリリース ノートに記載されています。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucm-dos>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Unified Communications Manager Session Management Edition を脆弱性のある製品として追加	概要、 該当製品	Final	2019 年 7 月 9 日
1.0	初回公開リリース	—	Final	2019 年 7 月 3 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、単独の転載や意識を施した場合、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。