Cisco Unified Communications製品における任意のファイル読み取りの脆弱性

アドバイザリーID : cisco-sa-cucm-imp-afr-YBFLNyzd
CVE-2022-20791
初公開日 : 2022-07-06 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCvz07265 CSCvz32980

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)、およびCisco Unified Communications Manager IM & Presence Service(Unified CM IM&P)のデータベースユーザ権限の脆弱性により、認証されたリモート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上で任意のファイルを読み取る可能性があります。

この脆弱性は、不十分なファイル権限の制限に起因します。攻撃者は、巧妙に細工されたコマンドをAPIからアプリケーションに送信することで、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、攻撃者は該当デバイスの基盤となるオペレーティングシステム上の任意のファイルを読み取る可能性があります。攻撃者がこの脆弱性を不正利用するには、有効なユーザクレデンシャルが必要です。

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-cucm-imp-afr-YBFLNyzd

該当製品

脆弱性のある製品

公開時点では、この脆弱性は次のシスコ製品のデフォルト設定に影響を与えていました。

- Unified CM
- Unified CM（SME）
- Unified CM IM&P

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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。

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

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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。 最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、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、およびこの脆弱性に対する修正を含むリリースを示しています。

Unified CMおよびUnified CM SME

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）
10.5	修正済みリリースに移行。
11.5	修正済みリリースに移行。
12.0	修正済みリリースに移行。

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）
12.5	修正済みリリースに移行。
14	14SU2

Unified CM IM&P

Cisco Unified CM IM&P リリース	First Fixed Release（修正された最初のリリース）
10.5	修正済みリリースに移行。
11.5	修正済みリリースに移行。
12.0	修正済みリリースに移行。
12.5	修正済みリリースに移行。
14	14SU2

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 は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

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

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-afr-YBFLNyzd

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	2022 年 7 月 6 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、単独の転載や意訳を施した場合、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。