Cisco TelePresence Collaboration EndpointおよびRoomOSソフトウェアの脆弱性

Medium	**アドバイザリーID :** cisco-sa-roomos-dkjGFgRK **初公開日 :** 2023-01-11 16:00 **最終更新日 :** 2023-03-07 14:21 **バージョン 1.1 :** Final **CVSSスコア :** 4.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwc47201 CSCwc85914	CVE-2023-20002 CVE-2023-20008

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 TelePresence Collaboration Endpoint(CE)ソフトウェアおよびCisco RoomOSソフトウェアの複数の脆弱性により、認証されたローカルの攻撃者が、該当デバイスを介してサーバ側の要求フォージェリ(SSRF)攻撃を実行したり、該当デバイスの任意のファイルを上書きしたりする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-roomos-dkjGFgRK

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性は次のシスコ製品に影響を与えました。

- TelePresence CEソフトウェア
- クラウドベースのクラウド対応オンプレミス運用のRoomOSソフトウェア

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、これらの脆弱性の影響を受けることが分かっています。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2023-20002:Cisco TelePresence CEおよびRoomOSソフトウェアのSSRF脆弱性

Cisco TelePresence CEおよびRoomOSソフトウェアの脆弱性により、認証されたローカルの攻撃者がアクセス制御をバイパスし、該当デバイスを介してSSRF攻撃を実行する可能性があります。

この脆弱性は、ユーザ入力の不適切な検証に起因します。攻撃者は、Webアプリケーションのユーザに巧妙に細工された要求を送信することで、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、攻撃者は該当システムから送信された任意のネットワーク要求を送信できる可能性があります。

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。

Bug ID:CSCwc85914
CVE ID：CVE-2023-20002
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.4
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE-2023-20008:Cisco TelePresence CEおよびRoomOSソフトウェアにおける任意のファイル書き込みの脆弱性

Cisco TelePresence CEおよびRoomOSソフトウェアのCLIの脆弱性により、認証されたローカル

攻撃者が該当デバイスのローカルシステム上の任意のファイルを上書きできる可能性があります。

この脆弱性は、ローカルファイルシステム内のファイルに対する不適切なアクセス制御に起因します。攻撃者は、該当デバイスのローカルファイルシステム上の特定の場所にシンボリックリンクを配置することで、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上の任意のファイルを上書きできる可能性があります。

注：この脆弱性は、Cisco DX70、DX80、TelePresence MXシリーズまたはTelePresence SXシリーズデバイスには影響を与えません。

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。

Bug ID:CSCwc47201
CVE ID：CVE-2023-20008
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.4
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N

回避策

これら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

シスコは、クラウドベースのCisco RoomOSソフトウェアでこれらの脆弱性に対処しています。ユーザの対処は必要ありません。サービス GUI のヘルプ機能を使用すると、現在の修復ステータスやソフトウェアバージョンを確認できます。その他の情報が必要な場合は、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。

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。

左の列にはシスコソフトウェアリリースが、右の列には、その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、およびこれらの脆弱性に対する修正を含むリリースが示されています。

CVE-2023-20002

Cisco TelePresence CEソフトウェアおよびRoomOSリリース	First Fixed Release（修正された最初のリリース）
9 ミリ秒	9.15.17 (Apr 2023)
10	10.19.4

CVE-2023-20008

Cisco TelePresence CEソフトウェアおよびRoomOSリリース	First Fixed Release（修正された最初のリリース）
9 ミリ秒	修正済みリリースに移行。
10	10.19.3.0

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とその公表は確認しておりません。

出典

CVE-2023-20002：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKyle Ossingerによる内部セキュリティテストで発見されました。

CVE-2023-20008：この脆弱性は、Cisco ASIGのDeklan Evansによる内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK

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	CVE-2023-20008の脆弱性のある製品情報を更新。CVE-2023-20002の修正済みリリース情報を更新。	詳細および修正済みリリース	Final	2023年3月7日
1.0	初回公開リリース	-	Final	2023年1月11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。