Cisco TelePresence コラボレーション エンドポイント、TelePresence Codec、RoomOS ソフトウェアで権限が昇格される脆弱性

High

アドバイザリーID : cisco-sa-20191106-telepres-roomos-privesc

初公開日 : 2019-11-06 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvq29901

CVE-2019-15288

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 コラボレーション エンドポイント（CE）、Cisco TelePresence Codec（TC）、および Cisco RoomOS ソフトウェアの CLI で脆弱性が確認されました。認証されたリモートからの攻撃者が、制限付きシェルのユーザ権限を無制限に昇格させる危険性があります。

この脆弱性は、入力に対する不十分な検証に起因します。 攻撃者は、影響を受けたデバイスへの SSH 接続をオープンするときに特定の引数を使用することで、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、攻撃者は影響を受けたデバイスの制限付きシェルに対して、無制限のユーザアクセス権を取得できます。

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ました。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-privesc

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、リリース 9.8.1 より前の Cisco TelePresence CE ソフトウェア、リリース 7.3.19 より前の Cisco TC ソフトウェア、およびリリース RoomOS September Drop 1 2019 より前の Cisco RoomOS ソフトウェアで SSH 機能が有効になっている場合です。

Cisco TelePresence CE ソフトウェア、Cisco TC ソフトウェア、および Cisco RoomOS ソフトウェアでは、SSH がデフォルトで有効になっています。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

回避策

この脆弱性に対処する回避策はありません。

SSH がデバイス管理で使用されていない場合は、SSH を無効にすることで、この脆弱性を緩和できます。 SSH を無効にする手順については、特定のエンドポイントのアドミニストレーション ガイドを参照してください。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。

ソフトウェアのアップグレードを検討する際には、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 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

Cisco TelePresence CE ソフトウェアリリース 9.8.1 以降および Cisco TC ソフトウェアリリース 7.3.19 では、この脆弱性は修正済みです。

Cisco TelePresence CE ソフトウェアおよび Cisco TC Software は、Software Center にアクセスし、次の手順でダウンロードできます。

1. [すべて参照（Browse all）] をクリックします。
2. [コラボレーション エンドポイント（Collaboration Endpoints）] を選択し、該当するエンドポイントを選択します。
3. [エンドポイント（Endpoint）] ページの左ペインからリリースにアクセスします。

クラウドベースの Cisco RoomOS September Drop 1 2019 サービスは、この脆弱性に対応済みです。 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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、シスコ内部でセキュリティテストを実施中、Cisco ASIG の KO によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-privesc

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 11 月 6 日

利用規約