Cisco Webex MeetingsおよびCisco Webex Meetings ServerのGhost Joinの脆弱性

Medium	**アドバイザリーID :** cisco-sa-webex-auth-token-3vg57A5r **初公開日 :** 2020-11-18 16:00 **最終更新日 :** 2020-12-10 16:10 **バージョン 1.4 :** Final **CVSSスコア :** 6.5 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvu42755 CSCvu42629	CVE-2020-3419

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 Webex MeetingsおよびCisco Webex Meetings Serverの脆弱性により、認証されていないリモートの攻撃者が、参加者リストに表示されずにWebexセッションに参加する可能性があります。

この脆弱性は、脆弱なWebexサイトによる認証トークンの不適切な処理に起因します。攻撃者は、脆弱性のある Cisco Webex Meetings または Cisco Webex Meetings Server サイトに偽造した要求を送信することで、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には、攻撃者がWebex会議に参加するためのアクセス権（該当する会議参加リンクとパスワードを含む）を持っている必要があります。攻撃者は、この脆弱性を不正利用して、参加者リストに表示されずに会議に参加し、音声、ビデオ、チャット、および画面共有機能に完全にアクセスできる可能性があります。

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-webex-auth-token-3vg57A5r

該当製品

脆弱性のある製品

この脆弱性は、2020年11月17日より前のすべてのCisco Webex Meetingsサイトに影響を与えました。Webex Meetingsはクラウドベースです。

公開時点では、この脆弱性はオンプレミスのCisco Webex Meetings Serverの次のリリースにも影響を与えました。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。

- 3.0MR3セキュリティパッチ4以前
- 4.0MR3セキュリティパッチ3以前

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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。

修正済みリリース

シスコは、クラウドベースのCisco Webex Meetingsサイトでこ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。

公開時点で、オンプレミスソフトウェアであるCisco Webex Meetings Serverの次のリリースには、この脆弱性に対する修正が含まれています。お客様には、更新されたソフトウェアリリースを適用することをお勧めします。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。

- 3.0MR3セキュリティパッチ5
- 4.0MR3セキュリティパッチ4

追加情報が必要なお客様は、Cisco TACまた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）は、この脆弱性の公表を確認しています。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

この脆弱性を報告していただいたIBM Researchの次の研究者に感謝いたします。

- Jiyong Jang氏(Research Scientist and Manager)
- Dhilung Kirat、研究科学者
- イアン・モロイ氏（RSM主席および部長）
- J.R. Rao、IBMフェロー、CTO

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-auth-token-3vg57A5r

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.4	3.0MRを3.0MR3に修正。	脆弱性が存在する製品	最終版	2020年12月10日
1.3	脆弱性のある製品および修正済みソフトウェアからモバイルアプリを削除。脆弱性のある製品および修正済みソフトウェアのフォーマットを更新。	「脆弱性のある製品」および「修正済みソフトウェア」	最終版	2020年11月23日
1.2	該当するソフトウェアリリースを更新。	脆弱性が存在する製品	最終版	2020年11月20日
1.1	研究者の名前を修正。	出典	最終版	2020年11月19日
1.0	初回公開リリース	—	最	2020

			終版	年 11 月 18 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。