Cisco Webex Meetingsサービスの HTTPキャッシュポイズニングの脆弱性

Medium

アドバイザリーID : cisco-sa-webex-cache-Q4xbkQBG
CVE-2025-20255
初公開日 : 2025-05-21 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwo66106

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のクライアント参加サービス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、会議参加サービス内でキャッシュされたHTTP応答を操作する可能性があります。

この脆弱性は、影響を受けるサービスに対する悪意のあるHTTP要求の不適切な処理に起因します。攻撃者は、HTTPキャッシュポイズニングとも呼ばれるサービス内に格納されたHTTP応答を操作することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はWebex Meetingsサービスからクライアントに対して不正なHTTP応答を返す可能性があります。

シスコはこの脆弱性に対処しており、オンプレミスのソフトウェアやデバイスをアップデートするためにお客様が何らかのアクションを行う必要はありません。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-webex-cache-Q4xbkQBG

該当製品

脆弱性のある製品

この脆弱性は、クラウドベースのCisco Webex Meetingsに影響します。

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

シスコは、クラウドベースのCisco Webex Meetings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。

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）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

シスコは、この脆弱性を報告していただいたMatthew B. Johnson(d3d)氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cache-Q4xbkQBG

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	2025年5月21日

利用規約

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。