

Cisco Webex Servicesのクロスサイトスクリプティングの脆弱性



アドバイザーID : cisco-sa-webex-xss-

7teQtFn8

初公開日 : 2025-05-21 16:00

バージョン 1.0 : Final

CVSSスコア : [6.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwo64795](#) [CSCwo64686](#)

[CSCwo64799](#)

[CVE-2025-](#)

[20250](#)

[CVE-2025-](#)

[20246](#)

[CVE-2025-](#)

[20247](#)

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の複数の脆弱性により、認証されていないリモートの攻撃者がクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

これらの脆弱性は、ユーザ入力の不適切なフィルタリングに起因します。攻撃者は、ユーザを悪意のあるリンクに誘導することで、これら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、攻撃者はターゲットユーザに対してクロスサイトスクリプティング攻撃を実行できる可能性があります。

シスコは本サービスでこれらの脆弱性に対処しており、お客様によるオンプレミスのソフトウェアやデバイスのアップデートは必要ありません。これらの脆弱性に対処する回避策はありません。

このアドバイザーは、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-xss-7teQtFn8>

該当製品

脆弱性のある製品

これらの脆弱性は、クラウドベースのCisco Webexに影響を与えます。

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。

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

シスコは、クラウドベースのCisco Webex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。

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とその公表は確認しておりません。

出典

シスコは、これらの脆弱性を報告していただいたPrasenjit Kanti Paul(BongHaxor)氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-7teQtFn8>

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

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、単独の転載や意識を施した場合、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。