Cisco Webexアプリの脆弱性

アドバイザリーID : cisco-sa-webex-app-ZjNm8X8j
初公開日 : 2024-07-17 16:00
バージョン 1.0 : Final
CVSSスコア : 6.4
回避策 : No workarounds available
Cisco バグ ID : CSCwj36947 CSCwj36943 CSCwj36941

CVE-2024-20396
CVE-2024-20395

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アプリケーションの複数の脆弱性により、認証されていない攻撃者が機密のクレデンシャル情報にアクセスでき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。アップデートはCisco Webexサービスの一部であり、これらのソフトウェアアップデートを入手するためにお客様が何らかの操作を行う必要はありません。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-app-ZjNm8X8j

該当製品

脆弱性のある製品

これらの脆弱性はCisco Webexアプリケーションに影響を与え、クラウドベースのCisco Webexサービスによって対処されました。

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-2024-20395:Cisco Webexアプリのセッショントークンの漏洩の脆弱性

Cisco Webexアプリケーションのメディア検索機能における脆弱性により、認証されていない隣接する攻撃者が機密セッション情報にアクセスできる可能性があります。

この脆弱性は、アプリケーションがイメージなどの組み込みメディアにアクセスする際に、バックエンドサービスへの要求が安全に送信されないことに起因します。攻撃者は、メッセージングサーバに格納されているメディアが埋め込まれたメッセージをターゲットユーザに送信することで、この脆弱性を不正利用する可能性があります。攻撃者が特権ネットワークの位置で送信トラフィックを観察できる場合、エクスプロイトに成功すると、安全に送信されていない要求からセッショントークン情報を取得し、取得したセッション情報を再利用してターゲットユーザとしてさらにアクションを実行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。

バグID: CSCwj36941、CSCwj36943
CVE ID：CVE-2024-20395
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.4
CVSSベクトル：CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

CVE-2024-20395:Cisco WebexアプリケーションのWindowsプロトコルハンドラにおけるクレデンシャル漏洩の脆弱性

Cisco Webexアプリのプロトコルハンドラの脆弱性により、認証されていないリモート攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、影響を受けるアプリケーションがファイルプロトコルハンドラを安全に処理できないことに起因します。攻撃者は、アプリケーションに要求を送信させるように設計されたリンクに従うようにユーザを誘導することで、この脆弱性を不正利用する可能性があります。攻撃者が特権ネットワークの位置で送信トラフィックを観察できる場合、エクスプロイトに成功すると、クレデンシャル情報などの機密情報を要求から取得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。

バグID:CSCwj36947
CVE ID：CVE-2024-20396
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

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Abicom社のCERT Michelian社およびYassine Bengana社のMaxime Escourbiac氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-ZjNm8X8j

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	2024年7月17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。