Cisco CX Cloud Agentの権限昇格の脆弱性

Medium	**アドバイザリーID :** cisco-sa-cxagent-gOq9QjqZ **初公開日 :** 2023-01-11 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.7 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwd51828 CSCwa73699	CVE-2023-20044 CVE-2023-20043

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 CX Cloud Agentの複数の脆弱性により、認証されたローカルの攻撃者が権限を昇格できる可能性があります。これらの脆弱性は、安全でないファイルアクセス許可が原因です。エクスプロイトに成功すると、攻撃者は該当デバイスを完全に制御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。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-cxagent-gOq9QjqZ

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco CX Cloud Agentに影響を及ぼしていました。

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。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。

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。

シスコは、リリース2.2より前のリリースをOpen Virtual Appliance(OVA)ファイルからインストールし、リリース2.2にアップグレードした場合、CVE-2023-20044がCisco CX Cloud Agentに影響を与えないことを確認しました。

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-2023-20043:Cisco CX Cloud Agentの権限昇格の脆弱性

Cisco CX Cloud Agentの脆弱性により、認証されたローカルの攻撃者が該当デバイスの権限を昇格できる可能性があります。この脆弱性は、安全でないファイルアクセス許可に起因します。攻撃者は、**sudo**コマンドを使用してスクリプトを呼び出すことにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスを完全に制御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。

Bug ID:CSCwa73699
CVE ID：CVE-2023-20043
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.7
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2023-20044:Cisco CX Cloud Agentの権限昇格の脆弱性

Cisco CX Cloud Agentの脆弱性により、認証されたローカルの攻撃者が該当デバイスの権限を昇格できる可能性があります。この脆弱性は、安全でないファイルアクセス許可に起因します。攻撃者は、テクニカルサポートに特定の設定を更新するよう説得することで、この脆弱性を不正利用する可能性があり、結果として安全でないスクリプトが呼び出される可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスを完全に制御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:CSCwd51828
CVE ID：CVE-2023-20044
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.7
CVSSベクトル：CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。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

発行時点では、次の表に記載されているリリース情報は正確でした。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。

左の列にはシスコソフトウェアリリースが、右の列には、そのリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含むリリースが示されています。

CVE-2023-20043

Cisco CX Cloud Agentリリース	First Fixed Release（修正された最初のリリース）
1.8 以前	1.9
1.8から2.2へのアップグレード	脆弱性なし
OVAファイルからインストールされた2.2	2.2.1
2.2.1	脆弱性なし

CVE-2023-20044

Cisco CX Cloud Agentリリース	First Fixed Release（修正された最初のリリース）
2 以前	2.2.1

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

この脆弱性は次のユーザによって発見されました。 カンスタンシン・マルケラウ シスコに対して行われます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cxagent-gOq9QjqZ

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	2023年1月11日

利用規約

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。