

Cisco Unified Intelligence Centerの脆弱性

Medium	アドバイザーID : cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	CVE-2023-20062
	初公開日 : 2023-03-01 16:00	CVE-2023-20061
	バージョン 1.0 : Final	CVE-2023-20061
	CVSSスコア : 6.5	CVE-2023-20061
	回避策 : No workarounds available	CVE-2023-20061
	Cisco バグ ID : CSCwd01184	
	CSCwd02972	

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 Unified Intelligence Centerの複数の脆弱性により、認証されたりリモートの攻撃者が機密情報を収集したり、該当システムに対してサーバ側の要求偽造(SSRF)攻撃を実行したりする可能性があります。

シスコでは、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する予定です。これらの脆弱性に対処する回避策はありません。

これらの脆弱性の詳細については本アドバイザーの「[詳細情報](#)」セクションを参照してください。

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-cuic-infodisc-ssrf-84ZBmwVk>

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はCisco Unified Intelligence Centerに影響を及ぼしていません。

Cisco Unified Intelligence Centerにバンドルされている次のシスコ製品も、これらの脆弱性の影響を受けます。

- Packaged Contact Center Enterprise (Packaged CCE)
- Unified Contact Center Enterprise(Unified CCE)
- Unified Contact Center Express (Unified CCX)

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。](#)

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-2023-20061: Cisco Unified Intelligence Centerの情報漏えいの脆弱性

Cisco Unified Intelligence CenterのWebベース管理インターフェイスの脆弱性により、認証されたリモートの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、特定のREST API出力の過剰な冗長性に起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、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に関連付けられたサービスのハッシュされたクレデンシャルを含む機密データを取得できる可能性があります。

シスコでは、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する予定です。この脆弱性に対処する回避策はありません。

バグID:CSCwd02972

CVE ID : CVE-2023-20061

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 6.5

CVSSベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2023-20062: Cisco Unified Intelligence Centerのサーバ側の要求偽造の脆弱性

Cisco Unified Intelligence Center(CUIC)のWebベース管理インターフェイスの脆弱性により、認証されたリモートの攻撃者がアクセスコントロールをバイパスし、該当システムでサーバ側の要

求フォージェリ(SSRF)攻撃を実行する可能性があります。

この脆弱性は、特定のHTTP要求に対する不適切な入力検証に起因します。攻撃者は、該当システムに巧妙に細工された HTTP 要求を送信することにより、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、攻撃者は該当システムから送信された任意のネットワーク要求を送信できる可能性があります。

シスコでは、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する予定です。この脆弱性に対処する回避策はありません。

バグID:CSCwd01184

CVE ID : CVE-2023-20062

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 5.0

CVSSベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N

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

[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、次の表に示す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。

左の列はシスコソフトウェアリリースを示し、右の列は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を示します。

Cisco Unified Intelligence Centerリリース	First Fixed Release (修正された最初のリリース)
12.5 以前	12.6(2) (2023年3月)
12.6	12.6(2) (2023年3月)

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セキュリティ研究者のKareem Mohamed氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk>

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3月1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。