Cisco Unified Intelligence Centerの権限昇格の脆弱性

アドバイザリーID : cisco-sa-cuis-priv-esc-3Pk96SU4
初公開日 : 2025-05-21 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : No workarounds available
Cisco バグ ID : CSCwk34893 CSCwk34894 CSCwk63233 CSCwk63223

CVE-2025-20113
CVE-2025-20114

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、認証されたリモートの攻撃者が該当システムで権限昇格攻撃を実行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-cuis-priv-esc-3Pk96SU4

該当製品

脆弱性のある製品

これらの脆弱性は、次のシスコソリューションの一部として使用されているかどうかなど、デバイスの設定に関係なく、Cisco Unified Intelligence Centerに影響を与えます。

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

これらの脆弱性は、Cisco Unified Contact Center Express(Unified CCX)にも影響を与えます。

これは、Cisco Unified CCXにはソフトウェアバンドルの一部としてCisco Unified Intelligence Centerが含まれているためです。

脆弱性が存在する Cisco ソフトウェア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。

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、これらの脆弱性がCisco Finesseには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-2025-20113:Cisco Unified Intelligence Centerの権限昇格の脆弱性

Cisco Unified Intelligence Center(CUIC)の脆弱性により、認証されたリモートの攻撃者が、該当システムの限定された機能セットに対する権限を管理者に昇格する可能性があります。

この脆弱性は、APIまたはHTTP要求におけるユーザ指定パラメータのサーバ側での検証が不十分であることに起因します。攻撃者は、巧妙に細工されたAPIまたはHTTP要求を該当システムに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、システムに格納されている機密情報の取得など、意図したアクセスレベルを超えてデータにアクセス、変更、または削除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:CSCwk34893およびCSCwk63233
CVE ID：CVE-2025-20113
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

CVE-2025-20114:Cisco Unified Intelligence Centerの水平権限昇格の脆弱性

Cisco Unified Intelligence Center(CUIC)のAPIの脆弱性により、認証されたリモートの攻撃者が、該当システムで水平権限昇格攻撃を実行できる可能性があります。

この脆弱性は、API要求のユーザ指定パラメータの検証が不十分であることに起因します。攻撃者は、巧妙に細工されたAPI要求を該当システムに送信して安全でないダイレクトオブジェクトリファレンス攻撃を実行することにより、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の異なるユーザに関連付けられている特定のデータにアクセス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:CSCwk34894 およびCSCwk63223
CVE ID：CVE-2025-20114
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。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最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

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	12.5(1)SU ES04
12.6	12.6(2)ES04
15	脆弱性なし

Cisco Unified CCXリリース	First Fixed Release（修正された最初のリリース）
12.5(1)SU3以前	修正済みリリースに移行。
15	脆弱性なし

シスコの 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済み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Spark Engineering ConsultantsのNoha Kany氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-priv-esc-3Pk96SU4

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

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。