Cisco Unified Contact Center Expressの脆弱性

Medium

アドバイザリーID : cisco-sa-uccx-multi-UhOTvPGL
初公開日 : 2025-06-04 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwk24068 CSCwk24130 CSCwk24108

CVE-2025-20276
CVE-2025-20277
CVE-2025-20279

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 Contact Center Express(Unified CCX)のWebベースの管理インターフェイスにおける複数の脆弱性により、認証されたリモートの攻撃者が、保存されたクロスサイトスクリプティング(XSS)攻撃を実行したり、該当デバイスで任意のコードを実行したりする可能性があります。これらの脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

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-uccx-multi-UhOTvPGL

該当製品

脆弱性のある製品

このドキュメントの発行時点で、これらの脆弱性はCisco Unified CCXに影響を与えました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2025-20279:Cisco Unified CCXストアドXSSの脆弱性

Cisco Unified CCXのWebベースの管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当システムでストアドXSS攻撃を実行できる可能性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、Webベースの管理インターフェイスへのユーザ入力の不適切なサニタイズに起因します。攻撃者は、悪意のあるスクリプトをインターフェイス経由で送信することで、こ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、攻撃者は該当システムでストアドXSS攻撃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: CSCwk24130
CVE ID：CVE-2025-20279
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVE-2025-20276:Cisco Unified CCXのリモートコード実行の脆弱性

Cisco Unified CCXのWebベースの管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が該当デバイスで任意のコードを実行できる可能性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、影響を受けるソフトウェアによるJavaオブジェクトの安全でないデシリアライゼーションに起因します。攻撃者は、巧妙に細工されたJavaオブジェクトを該当デバイス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、攻撃者は権限の低いユーザとして、該当デバイスの基盤となるオペレーティングシステムで任意のコードを実行でき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、root権限に昇

格するためのさらなるアクションを実行できるようになります。

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: CSCwk24108
CVE ID：CVE-2025-20276
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：3.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

CVE-2025-20277:Cisco Unified CCXのパストラバーサルの脆弱性

Cisco Unified CCXのWebベースの管理インターフェイスにおける脆弱性により、認証されたローカル攻撃者が該当デバイスで任意のコードを実行できる可能性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、制限されたディレクトリへのパス名の不適切な制限（パストラバーサル）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Web要求を送信し、SSHセッションを介して特定のコマンドを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は権限の低いユーザとして、該当デバイスの基盤となるオペレーティングシステムで任意のコードを実行でき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、root権限に昇格するためのさらなるアクションを実行できるようになります。

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: CSCwk24068
CVE ID：CVE-2025-20277
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：3.4
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/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。

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。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された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。

Cisco Unified CCX リリース	First Fixed Release（修正された最初のリリース）
15.0 より前	修正済みリリースに移行。
15.0	15.0(1)

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NATO Cyber Security Center(NCSC)のAntonin B.氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-multi-UhOTvPGL

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6月4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。