# Cisco Unified Contact Center Expressにおけるリモートでのコード実行の脆弱性


アドバイザリーID : cisco-sa-cc-unauth-rce-QeN8h7mQ
初公開日 : 2025-11-05 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCwq36528 CSCwq36573

CVE-2025-20354
CVE-2025-20358

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Java Remote Method Invocation(RMI)プロセスにおける複数の脆弱性により、認証されていないリモートの攻撃者が、任意のファイルをアップロードし、認証をバイパスし、任意のコマンドを実行し、権限をrootに昇格す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-cc-unauth-rce-QeN8h7mQ

## 該当製品

### 脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco Unified CCXに影響を与えます。

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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

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

## 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。

脆弱性の詳細は以下のとおりです。

CVE-2025-20354:Cisco Unified CCXのリモートコード実行の脆弱性

Cisco Unified CCXのJava Remote Method Invocation(RMI)プロセスにおける脆弱性により、認証されていないリモートの攻撃者が、該当システムでルート権限を使用して任意のファイルをアップロードし、任意のコマンドを実行する可能性があります。

この脆弱性は、特定のCisco Unified CCX機能に関連する認証メカニズムが不適切なことに起因します。攻撃者は、Java RMIプロセスを介して該当システムに巧妙に細工されたファイルをアップロードすることにより、この脆弱性を不正利用する可能性があります。エクスプロイトが成功すると、攻撃者が基盤となるオペレーティング システムで任意のコマンドを実行し、特権をルートに昇格できる危険性があります。

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: CSCwq36528
CVE ID：CVE-2025-20354
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2025-20358:Cisco Unified CCXエディタの認証バイパスの脆弱性

Cisco Unified CCXのContact Center Express(CCX)Editorアプリケーションの脆弱性により、認証されていないリモートの攻撃者が認証をバイパスし、スクリプトの作成と実行に関する管理アクセス許可を取得する可能性があります。

この脆弱性は、CCX Editorと該当するUnified CCXサーバ間の通信における認証メカニズムが不適切なことに起因します。攻撃者は、認証フローを悪意のあるサーバにリダイレクトし、認証が成功したと思い込ませることにより、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、影響を受けるUnified CCXサーバの基盤となるオペレーティングシステムで、内部非rootユーザアカウントとして任意のスクリプトを作成し、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: CSCwq36573
CVE ID：CVE-2025-20358
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.4
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

## 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

シスコでは、回避策や緩和策は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

### 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 CCX リリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 12.5 SU3以前 | 12.5 SU3 ES07 |
| 15.0 | 15.0 ES01 |

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セキュリティ研究者のJahmel Harris氏に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-unauth-rce-QeN8h7mQ

## 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11月5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。