Cisco Packaged Contact Center EnterpriseおよびCisco Unified Contact Center Enterpriseのクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-ucce-pcce-xss-2JVyg3uD
初公開日 : 2026-01-21 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 : CSCwr61043 CSCwp27481

CVE-2026-20109
CVE-2026-20055

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 Packaged Contact Center Enterprise(Packaged CCE)およびCisco Unified Contact Center Enterprise(Unified CCE)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、該当デバイスのWebベースの管理インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスがユーザ入力を適切に検証しないことに起因しています。攻撃者は、悪意のあるコードをインターフェイスの特定のページに挿入することで、これら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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセス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。

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-ucce-pcce-xss-2JVyg3uD

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はデバイス設定に関係なく、Cisco Packaged CCEおよびCisco Unified CCEに影響を与えていました。

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。

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。

- Unified Customer Voice Portal（CVP）
- Cisco Unified Intelligence Center（CUIC）
- Virtualized Voice Browser

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、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、回避策や緩和策（適用可能な場合）を一時的な解決策と見なします。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

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。

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。中央および右の列は、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。

Cisco Packaged CCEおよびUnified CCEリリース	CVE-2026-20055 の最初の修正済みリリース	CVE-2026-20109 の最初の修正済みリリース
12.6 より前	修正済みリリースに移行。	修正済みリリースに移行。
12.6	12.6(2)_ES101	修正済みリリースに移行。
15.0	15.0(1)ES202511	15.0(1)ES202511

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

この脆弱性は、シスコ内部でのシステム セキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-xss-2JVyg3uD

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	2026年1月21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。