

Cisco Enterprise ChatおよびEメールストアドロスサイトスクリプティングの脆弱性



アドバイザーID : cisco-sa-ece-xss-

CbtKtEYc

初公開日 : 2025-07-02 16:00

バージョン 1.0 : Final

CVSSスコア : [6.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwo21879](#)

[CVE-2025-](#)

[20310](#)

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 Enterprise Chat and Email(ECE)のWeb UIの脆弱性により、認証されていないリモートの攻撃者がインターフェイスのユーザに対してストアド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。

この脆弱性は、Web UI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、この脆弱性を不正利用して、巧妙に細工されたリンクをクリックするようにインターフェイスのユーザを誘導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。この脆弱性を不正利用するには、攻撃者は有効なエージェントクレデンシャルを必要とします。

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。この脆弱性に対処する緩和策があります。

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-ece-xss-CbtKtEYc>

該当製品

脆弱性のある製品

公開時点で、リッチテキストコンテンツポリシーのインバウンドEメールセキュリティポリシーが無効になっているCisco ECEがこの脆弱性の影響を受けました。

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。

リッチテキストコンテンツポリシー設定の決定

Cisco ECEサーバのリッチテキストコンテンツポリシーの受信電子メールセキュリティポリシー設定のステータスを確認するには、ECE System Console(ESC)またはCisco Packaged Contact Center Enterprise(PCCE)のSingle Pane of Glass(SPOG)に接続し、Digital Channels > Chat and Email > Partition > Security > Rich Text Content Policyの順に選択します。

受信電子メールセキュリティポリシー設定が有効になっている場合、システムはこの脆弱性の影響を受けません。この設定が無効になっている場合、システムはこの脆弱性の影響を受けます。

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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

回避策

この脆弱性に対処する回避策はありません。ただし、Cisco ECEサーバのリッチテキストコンテンツポリシーの受信電子メールセキュリティポリシー設定を有効にすると、この脆弱性は緩和されます。

この設定を有効にするには、UCCEシステムコンソールに接続し、Digital Channels > Chat and Email > Partition > Security > Rich Text Content Policyの順に選択します。受信電子メールセキュリティポリシーの設定を有効に変更します。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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 ECE リリース	First Fixed Release (修正された最初のリリース)
11	修正済みリリースに移行。
12	12.6(1)_ES11
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やその公表は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-xss-CbtKtEYc>

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7月2日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。