# Cisco Unified CallManager Webインターフェイス 入力 ValidationÂ バイパス の 脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** Cisco-SA-20070523-CVE-2007-2832<br>**初公開日 :** 2007-05-23 16:43<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 1.9<br>**回避策 :** Yes<br>**Cisco バグ ID :** | CVE-2007-2832 |

**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 CallManagerバージョン 4.3(1) および前は非認証を可能にする可能性があるセキュリティ制限をバイパスし、クロスサイト スクリプティング攻撃を行なうために脆弱性リモート攻撃者が含まれています。

CallManager Webインターフェイス Search 形式がユーザが指定する入力の不十分な sanitization に原因でこの脆弱性存在。 非認証はユーザの悪意のあるリンクに従うように確信によって、リモート攻撃者この脆弱性を不正利用する可能性があります。 この操作は攻撃者がユーザーのブラウザー セッション内の任意 HTML コードを実行することを可能にする可能性があります。

機能 URL は共用利用可能です。

Cisco はセキュリティ応答のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

攻撃者はユーザー操作にエクスプロイトを達成するために頼ります。 攻撃者はユーザを多分 E メールか他のメッセージ の タイプの一部として提供される悪意のある URL に、続くように確信させる必要があります。 悪意のあるリンクに従うことによって、攻撃者はユーザーのブラウザーセッションの任意 HTML コードを実行する可能性があります。 外付け フラッシュか、スクリプトを書くか、または他のアクティブ コンテンツを参照するのに攻撃者が HTML 要素を使用できるので攻撃者は設定によって多分ユーザーのブラウザー内のスクリプトを、実行する可能性があります。 そのようなスクリプトは最近提出されたブラウザ 情報か他の機密 情報を回復 する可能性があります。

サーバ側の入力はベンダーから以降のバージョンの不正 なコードのインジェクトを防ぐために改善されました。

ベンダーはまたこのタイプの不正利用がバージョン 4.2(3)SR2 および それ 以上の Webアプリケーション ファイアウォールによって現在ブロックされることを示しました。

### 該当製品

## 修正済みソフトウェア

Cisco CallManagerバージョン 4.3(1) および前は脆弱です。

## 脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

### 改訂履歴

| バージョン | 説明 | Section | ステータス | 日付 |
|---|---|---|---|---|
| 1.0 | 初版リリース | 該当なし | Final | 2007-May-23 |

### 利用規約