Cisco CallManager Administration およびユーザ OptionsÂ Webインターフェイス クロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20060619-CVE-2006-3109 **初公開日 :** 2006-06-19 23:41 **最終更新日 :** 2015-01-31 08:30 **バージョン 2.0 :** Final **CVSSスコア :** 1.9 **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-3109

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

4.3(1)、4.2(3)、4.1(3)SR4 および 3.3(5)SR3 以前の Cisco CallManagerバージョンは非認証を可能にする可能性があるユーザーのブラウザー セッションの任意スクリプトを実行するために脆弱性がリモート攻撃者含まれています。

CallManagerアドミニストレーションのWeb インターフェイスおよび CallManager ユーザー オプション Webインターフェイスの不適当な入力 sanitization による脆弱性存在。 攻撃者はユーザの設計されているリンクに従うように確信によって脆弱 な パラメータに悪意のあるスクリプト コードを渡すように脆弱性を不正利用する可能性があります。 これは攻撃者が影響を受けたサイトという点においてユーザーのブラウザー セッションの任意スクリプト コードを実行することを可能にする可能性があります。

プルーフ オブ コンセプト コードは利用できます。

Cisco はセキュリティ応答のこの脆弱性を確認しましたが、パッチはまだ利用できません。

この脆弱性を不正利用するために、攻撃者は影響を受けた CallManager Server のための IP アドレスおよびポート番号がなければなりません。 これは社会工学か内部攻撃者をほとんどの場合必要とします。 ただし脆弱 な インターフェイスがインターネット--に直接さらされれば、攻撃者はアドレスを確認する可能性があります。 攻撃者は依然としてこれらのシステムの 1 つのユー

ザを巧妙に細工された リンクを実行するように確信させる必要があります。

該当製品

修正済みソフトウェア

以下は脆弱です:

Cisco Unified CallManager 4.3(1)
4.2(3.1) 前の Cisco Unified CallManager 4.2
4.1(3)SR4 前の Cisco Unified CallManager 4.1
3.3(5)SR3 以前の Cisco CallManager 3.3
Cisco CallManager 3.2 およびそれ以降
Cisco CallManager 3.1 およびそれ以降

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	2006-Jun-19

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。