Cisco Unified MeetingPlace テンプレート 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-20070808-CVE-2007-4284 **初公開日 :** 2007-08-08 16:55 **バージョン 1.0 :** Final **CVSSスコア :** 1.9 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-4284

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

5.3.235.0 以前の Cisco Unified MeetingPlace バージョンは非認証を可能にする可能性があるクロスサイト スクリプティング攻撃を行なうために脆弱性がリモート攻撃者含まれています。

Cisco Unified MeetingPlace によってパラメータの不十分なフィルタリングによるこの脆弱性存在。 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。 従われたとき、リンクは Cisco Unified MeetingPlace サイトのセキュリティ コンテキストのユーザーのブラウザー セッション内の任意スクリプト コードまたは HTML の実行を引き起こす可能性があります。

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。

この脆弱性を不正利用するために、攻撃者はユーザを多分電子メール メッセージの内で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。 エクスプロイト前に、ユーザは影響を受けたアプリケーションに有効な、ログイン した セッションまたはエクスプロイト試みの一部としてログインがなければなりません。 不正利用の成功の結果として、攻撃者は Cisco Unified MeetingPlace アプリケーション内のユーザーのブラウザー セッションの任意スクリプト コードを実行する可能性があります。 エクスプロイトは攻撃者が敏感なブラウザ ベースの情報へのアクセス権を得るか、または可能性のある ユーザとして影響を受けたサイトの処置をとることを可能にする可能性があります。

ソフトウェア バージョン 5.3.333.0 およびそれ以降はきちんとフォーマットされていた XML メッセージを返すために訂正されました。

該当製品

修正済みソフトウェア

5.3.235.0 以前の Cisco Unified MeetingPlace バージョンは脆弱です。

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-Aug-08

利用規約