Cisco Unified MeetingPlace Login 画面 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-20071107-CVE-2007-5581 **初公開日 :** 2007-11-07 14:56 **最終更新日 :** 2012-07-14 19:33 **バージョン 2.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-5581

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 Unified MeetingPlace バージョン 5.3.235.0 および前、5.4 および 6.0 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。

この脆弱性は Cisco Unified MeetingPlace の Login 形式に通じるパラメータの不十分なフィルタリングが原因です。 非認証はユーザの悪意のあるパラメータが含まれている URL に続く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、リンクにより影響を受けたサイトは影響を受けたサイトのセキュリティ コンテキスト内の影響を受けたユーザに攻撃者供給されたスクリプト コードを戻します可能性があります。 これは攻撃者がユーザーのブラウザー セッション内の任意スクリプト コードか HTML を実行することを可能に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への敏感なブラウザ関連情報へのアクセス権を得ることを可能にする可能性があります。

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メッセージングの電子メール メッセージか他の形式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。 エクスプロイトは攻撃者が 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 コードを実行することを可能に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。

顧客と組織の展開会合場所間のリモート Web 会合を促進するために影響を受けた Login 形式は頻繁に配置されるのでこれらのシステムのユーザを巧妙に細工されたリンクに従うように確信させるように攻撃者のためにとるに足らないかもしれません。 ただし、アプリケーションの性質が原因で、情報の種類は攻撃者表わされた場合表われられますその性質に制限され、深刻な脅威を与えてまずないですかもしれません。

Ciscoセキュリティ応答は追加バグID および技術情報とアップデートされ、追加更新済ソフトウェアはリリースされました。 管理者はバグID が両方とも十分にこの脆弱性を解決することができるように提供される修正を設定するように助言されます。

該当製品

Cisco は次のリンクで Cisco バグ ID CSCsk17122 および CSCth13602 をアドレス指定するためにセキュリティ応答をリリースしました: cisco-sr-20071107-mp

脆弱性のある製品

Cisco Unified MeetingPlace バージョン 5.3.235.0 および前、5.4 および 6.0 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。

回避策

管理者は適切な更新を加えるように助言されます。

ユーザは信頼できない Webサイトを参照しないように助言されます。

ユーザは信頼できないソースからの E メールを開かないように助言されます。

ユーザは非請求リンクに従わないように助言されます。 ユーザはそれに続く前に信頼されたソースからの予想外リンクの信頼性を確認する必要があります。

Cisco によって加えられる知性チームからの次に挙げるドキュメントは識別を管理者に指示でき、軽減は更新済ソフトウェアを加える前にこの脆弱性を不正利用するように試みます:
クロスサイト スクリプティング 脅威ベクターの概要

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは

tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20071107-CVE-2007-5581

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2007-Nov-07

利用規約