Cisco Unified MeetingPlace XSS の脆弱性

Inform ational

アドバイザリーID : cisco-sa-20071107-mp
初公開日 : 2007-11-07 13:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

これは、Joren McReynoldsがCisco Unified MeetingPlace Web Conferencingのクロスサイトスクリプティング(XSS)の脆弱性に関して発見し、シスコに報告した問題に対するCisco PSIRTの応答です。

元のレポートは、次のリンク先で入手できます。http://secunia.com/advisories/26462/

セキュリティの脆弱性に関して研究者と協力し、製品レポートのレビューと支援を行う機会を歓迎いたします。

この脆弱性は、Cisco Bug ID CSCsk17122 (登録ユーザ専用)に記載されています。

シスコがこの応答を公開して以来、*FirstName*または*LastName*パラメータに関連付けられた他のバリエーションのXSSが検出されています。これらの追加のXSS脆弱性は、Cisco Bug ID CSCth13602 (登録ユーザ専用)に記載されています。

XSSの脆弱性を完全に修正するには、両方のCisco Bug IDの修正が必要です。

このCisco Security Responseは、次のリンクに掲載されています。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071107-mp

本脆弱性の ID は CVE ID CVE-2007-5581 です。

追加情報

Cisco Unified MeetingPlace Web Conferencing(MeetingPlace)は、組織のイントラネットおよび工

クストラネットにリアルタイムコラボレーション機能を提供し、MeetingPlaceとWebサーバを統合して、ブラウザベースのインターフェイスをユーザに提供します。Web Conferencingを使用すると、ユーザは会議のスケジュール設定や会議への参加、会議資料へのアクセス、一般的なWebブラウザからのドキュメントのコラボレーションを行うことができます。

MeetingPlaceは、ログイン画面からのクロスサイトスクリプティング(XSS)攻撃に対して脆弱です。このXSSの脆弱性が不正利用されると、悪意のあるコードまたはスクリプトがURLに埋め込まれ、FirstNameまたはLastNameパラメータに関連付けられます。

悪意のあるコードは通常、リンクのURLに埋め込まれたスクリプトの形式をとります。悪意のあるコードは、脆弱なサーバまたは悪意のあるWebサイトに保存されている可能性もあります。攻撃者は、悪意のあるコードをユーザのブラウザに注入（反映）する脆弱なMeetingPlaceサーバへの悪意のあるリンクを疑いを持たないユーザに従わせようとします。

回避策

この脆弱性に対する回避策はありません。シスコでは、この脆弱性に対処するためにホットフィックスを適用することを推奨しています。

影響を受けるソフトウェア バージョン	ホットフィックス – CSCsk17122	ホットフィックス – CSCth13602
5.3以前のバージョン	該当。ホットフィックスはありません。	
5.4	5.4.156.2E	該当。ホットフィックスはありません。
6.0	6.0.244.1A	6.0.639.10

Â

XSS攻撃と、これらの脆弱性を悪用するために使用される方法の詳細については、次のリンクにあるCisco Applied Intelligence Responseの『Understanding Cross-Site Scripting (XSS) Threat Vectors』を参照してください。

http://www.cisco.com/warp/public/707/cisco-air-20060922-understanding-xss.shtml

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の

説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071107-mp

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.1	Cisco Bug ID **CSCth13602**の詳細を追加。		2010年7月8日
リビジョン 1.0	初回公開リリース		2007年11月7日

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。

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。