Cisco WebEx Meetings Serverのユーザ列挙の脆弱性

Medium

アドバイザリーID : Cisco-SA-20140728-CVE-2014-3286
初公開日 : 2014-07-28 20:00
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuj81744 CSCuj81665 CSCuj81655 CSCuj81688 CSCuj81685 CSCuj81661

CVE-2014-3286

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 WebEx Meetings ServerのWebフレームワークの脆弱性により、認証されていないリモートの攻撃者が有効なユーザアカウントを列挙できる可能性があります。

この脆弱性は、返されたメッセージの不適切なサニタイズに起因します。攻撃者は、巧妙に細工されたURL要求を該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。

シスコはセキュリティ通知で脆弱性を確認していますが、ソフトウェアアップデートは提供されていません。

この脆弱性を不正利用するために、攻撃者は、悪意のあるサイトにユーザを誘導するためのリンクを提供したり、誤解させる言葉や指示を使用して、提供されたリンクに進むようにユーザを促す可能性があります。

該当製品

影響を受ける製品バージョンの一覧については、Cisco Bug ID CSCuj81685、CSCuj81688、CSCuj81665、CSCuj81744、CSCuj81661、およびCSCuj81655を参照してください。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco WebEx Meetings Serverバージョン1.5に脆

弱性が存在します。Cisco WebEx Meetings Serverのこれ以降のリリースにも脆弱性が存在する可能性があります。

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

今後のアップデートやリリースについては、ベンダーに問い合わせることをお勧めします。

ユーザは、非要請リンクが安全に追跡できることを確認する必要があります。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20140728-CVE-2014-3286

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2014年7月28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。