Cisco WebEx Meetings Serverにおけるコマンドインジェクションの脆弱性

Critical

アドバイザリーID : cisco-sa-20150204-wbx CVE-2015-0589
初公開日 : 2015-02-04 16:00
バージョン 1.0 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuj40460

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の管理Webインターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当システムおよび該当システムによって管理されるデバイスで任意のコマンドを実行する可能性があります。

この脆弱性は、不適切なユーザ入力の検証に起因します。攻撃者は、Webインターフェイスの影響を受けるフィールドに入力を巧妙に細工することで、この脆弱性を不正利用する可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。これらの脆弱性に対しては回避策がありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150204-wbx

該当製品

脆弱性のある製品

このアドバイザリで公開されている脆弱性は、Cisco WebEx Meetings Serverに影響を与えます。次のバージョンのCisco WebEx Meetings Serverがこの脆弱性の影響を受けます。

- Cisco WebEx Meetings Serverバージョン1.0
- Cisco WebEx Meetings Serverバージョン1.1
- Cisco WebEx Meetings Serverバージョン1.5

脆弱性を含んでいないことが確認された製品

次の製品およびバージョンは、この脆弱性の影響を受けません。

- Cisco WebExクラウドサービス
- Cisco WebEx Meetings Server 2.0
- Cisco WebEx Meetings Server 2.5

詳細

Cisco WebEx Meetings Serverは、オンプレミス会議サーバ向けの仮想化されたソフトウェアベースのソリューションです。

Cisco WebEx Meetings Serverの管理Webインターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当システムおよび該当システムによって管理されるデバイスで任意のコマンドを実行する可能性があります。

この脆弱性は、不適切なユーザ入力の検証に起因します。攻撃者は、Webインターフェイスの影響を受けるフィールドに入力を巧妙に細工することで、この脆弱性を不正利用する可能性があります。Cisco WebEx Meetings Serverのコマンドインジェクションの脆弱性が不正利用されると、攻撃者がルートユーザとして基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

この脆弱性は、Cisco Bug ID CSCuj40460(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2015-0589が割り当てられています

回避策

この脆弱性に対する回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

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-20150204-wbx

改訂履歴

リビジョン 1.0	2015年2月4日	初版リリース

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。