

# Cisco WebEx ブラウザ拡張機能リモート コード実行の脆弱性

**Critical**    アドバイザリーID : cisco-sa-[CVE-2017-0717-webex](#)  
初公開日 : 2017-07-17 16:00    [2017-6753](#)  
最終更新日 : 2017-08-11 15:41  
バージョン 1.3 : Final  
CVSSスコア : [9.6](#)  
回避策 : [Yes](#)  
Cisco バグ ID : [CSCvf15030](#) ,  
[CSCvf15020](#) , [CSCvf15033](#) ,  
[CSCvf15012](#) , [CSCvf15036](#) ,  
[CSCvf15037](#)

**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

Google Chrome および Mozilla Firefox 向け Cisco WebEx ブラウザ拡張機能の脆弱性により、認証されていないリモートの攻撃者が、被侵害システム上の被侵害ブラウザの権限を使用して任意のコードを実行する可能性があります。この脆弱性は、Microsoft Windows で動作している Cisco WebEx Meetings Server、Cisco WebEx Center ( Meeting Center、Event Center、Training Center、Support Center )、Cisco WebEx Meetings のブラウザ拡張機能に影響します。

この脆弱性は、拡張機能の設計に欠陥があることに起因します。被侵害ユーザが被侵害ブラウザで、攻撃者の制御する Web ページを参照したり攻撃者の提供したリンクをたどったりするよう誘導された場合、この脆弱性が悪用される可能性があります。成功すると、攻撃者は被侵害ブラウザの権限を使用して任意のコードを実行することができます。

シスコは、Google Chrome および Mozilla Firefox 向けに、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ました。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170717-webex>

## 該当製品

# 修正済みソフトウェア

この脆弱性は、Windows 向けの Cisco WebEx 拡張機能に影響し、サポートされているほとんどのブラウザが対象になります。影響を受けるブラウザは Google Chrome および Mozilla Firefox です。

このドキュメントで説明する脆弱性の影響を受ける Cisco WebEx ブラウザ拡張機能のバージョンは、次のとおりです。

- Google Chrome 向け Cisco WebEx 拡張機能の、1.0.12 より前のバージョン
- Mozilla Firefox 向け Cisco WebEx 拡張機能の、1.0.12 より前のバージョン

使用されている Cisco WebEx 拡張のバージョンは、次の手順を使用して確認できます。

## Google Chrome

Chrome ユーザの場合、Google Chrome 向け Cisco WebEx 拡張機能のバージョンを確認するには、以下の手順を実行します。

1. Chrome 3 [ (Tools) ] > [ 拡張機能 (Extensions) ]

拡張機能のバージョンは、Cisco WebEx 拡張機能の名前の隣に表示されます。

Google Chrome 向け Cisco WebEx 拡張機能の ID スtring ( この String を使用して拡張機能を含むホストを特定することができます ) は次のとおりです。

*jlhmfmgfeifomenelglieieghnjghma* **Mozilla Firefox**

Firefox ユーザの場合、Mozilla Firefox 向け Cisco WebEx 拡張機能のバージョンを確認するには、以下の手順を実行します。

1. 3 [ (Add-ons) ]
2. **拡張機能** タブをクリックして下さい
3. 拡張機能のリストから [Cisco WebEx 拡張機能 ( Cisco WebEx Extension ) ] を見つけて [詳細 ( More ) ] リンクをクリックすると、バージョン情報が表示されます。

## 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。

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco WebEx Productivity Tools
- Mac、Linux 向け Cisco WebEx ブラウザ拡張
- Microsoft Edge、Internet Explorer の Cisco WebEx

## 改訂履歴

Version	Description	Section	Status	日付
1.3	Cisco WebEx Meetings Server バージョン 2.6 用パッチについての情報が含まれていません。	修正済みソフトウェア	Final	2017-August-11
1.2	ブラウザの自動更新に関する情報を追加	修正済みソフトウェア	Final	2017-July-19
1.1	回避策のセクションを変更	回避策	Final	2017-July-18
1.0	Initial public release.		Final	2017-July-17

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。