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-20170717-webex

初公開日 : 2017-07-17 16:00

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 : No workarounds available

Cisco バグ ID : CSCvf15030 CSCvf15020 CSCvf15033 CSCvf15012 CSCvf15036 CSCvf15037

CVE-2017-6753

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

脆弱性のある製品

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 ストリング（このストリング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。
jlhmfgmfgeifomenelglieieghnjghma **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

侵害のインジケーター

回避策

この脆弱性に対処する回避策はありません。 ただし、Windows ユーザは Internet Explorer を、Windows 10 システムの管理者とユーザは Microsoft Edge を使用して WebEx セッションに参加できます。Microsoft Internet Explorer と Microsoft Edge はこの脆弱性の影響を受けません。 さらに、管理者およびユーザは Windows システムから会合サービス取り外しツールの DOC-2672 から利用可能である使用によってすべての WebEx ソフトウェアを取除くことができます。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

脆弱性を解決するため、次に示す最新版を使用していることを確認する必要があります。

1. Google Chrome または Mozilla Firefox 向け Cisco WebEx 拡張機能
2. Cisco WebEx デスクトップ アプリケーション

次の製品の修正に関する最新情報については、以下の該当する Cisco Bug ID を参照してください。

- Cisco WebEx Meeting Center： CSCvf15012
- Cisco WebEx Event Center： CSCvf15036
- Cisco WebEx Training Center： CSCvf15033
- Cisco WebEx Support Center： CSCvf15037
- Cisco WebEx Meetings Server： CSCvf15020
- Cisco WebEx Meetings： CSCvf15030

ブラウザ更新

以下のサブセクションでは Cisco WebEx ブラウザ拡張機能を更新する手順について説明します。ブラウザを起動してウィンドウを 3 ~ 6 時間開いたままにしておくことで、ブラウザの拡張機能を自動更新できます。拡張機能はこの間に自動更新されます。

注: 自動更新の確認が完了する前にブラウザのウィンドウを閉じると、タイマーがリセットされます。自動更新するには、ブラウザ ウィンドウをもう一度開き、3 ~ 6 時間閉じないでおく必要があります。

Google Chrome

Google Chrome 向け Cisco WebEx 拡張機能のバージョン 1.0.12 は 2017 年 7 月 13 日にリリースされました。このバージョンには、この脆弱性に対する修正が含まれています。 Chrome ユーザの場合、Google Chrome 向け Cisco WebEx 拡張機能の修正バージョンが使用されているか確認するには、以下の手順を実行します。

1. Chrome で、menu ボタン (アプリケーションの甲革権利の 3 つの点) をクリックし、**ツール > 拡張機能を**『More』 を選択 して下さい。
2. 拡張機能マネージャの上で**開発者 Mode チェックボックスを**チェックして下さい。 Chrome にボタンの行が表示されます。
3. **アップデート 拡張機能 Now ボタンを**クリックして下さい。
4. Chrome ブラウザを再起動します。

Mozilla Firefox

Mozilla Firefox 向け Cisco WebEx 拡張機能のバージョン 1.0.12 は 2017 年 7 月 12 日にリリースされました。このバージョンには、この脆弱性に対する修正が含まれています。 Firefox ユーザの場合、Mozilla Firefox 向け Cisco WebEx 拡張機能の修正バージョンが使用されているか確認するには、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。
4. はめば歯車を検索バーの隣でクリックし、**確認します更新があるように**選択して下さい

Microsoft Internet Explorer

Google Chrome、Mozilla Firefox、Internet Explorer には共有コンポーネントが存在するため、Internet Explorer ユーザは Cisco WebEx プラグインを更新するよう求められます。 プラグインは、各 WebEx 製品に関連する Cisco WebEx クライアント パッケージの一部として利用可能で、WebEx サイトが修正バージョンにアップグレードされた後にダウンロードできます。 アップグレードされたクライアントはアップグレードが実行された後各サイトの **ダウンロード** セクションから利用できます。 更新済みクライアント ソフトウェアのないアップグレード済みサイトに接続しているユーザの場合、オンライン アップグレードの実行を促す指示が出ることがあります。

Microsoft Internet Explorer 向けブラウザ プラグインが正しくアップグレードできたかどうかは、次の手順を使用して確認できます。

注: Internet Explorer におけるプラグインの登録名は、プラグインに使用するインストール方法に基づいて異なる可能性があります。 プラグインのバージョンは、アップデートを提供した Cisco WebEx のバージョンによって異なります。 アップデートは、WebEx ミーティング参加時に Web 経由で適用されているか、または MSI ファイル経由でクライアントのローカル アップデートによって適用されている可能性があります。 あるバージョンの Cisco WebEx からの修正バージョン プラグインをインストールすると、それ以外の修正バージョンの Cisco WebEx によってインストールされるバージョンにダウングレードしたり変更したりすることはできません。 Internet Explorer ユーザの場合、Internet Explorer 向けのプラグインの修正バージョンが使用されているか確認するには、次の手順を実行します。

1. Internet Explorer の [ツール（Tools）] ボタン（アプリケーションの右上の歯車アイコン）をクリックして、[アドオンの管理（Manage add-ons）] を選択します。
2. [表示（Show）] ドロップダウン メニューから、[すべてのアドオン（All add-ons）] を選択します。
3. **Cisco WebEx LLC** の下で**ダウンロード マネージャ**か **GpcContainer クラス**追加項目を選択して下さい。 バージョン番号は**管理追加項目**ウィンドウの下部のので表示する。
4. 表示する**ダウンロード マネージャバージョン**か **GpcContainer クラス** バージョンが次 の テーブルのバージョン ストリングの 1 つであること検証して下さい:

Cisco WebEx Major Version	Fixed GPC Container or Download Manager Version
32.3.4.5	10032.3.2017.711
31.14.3.30	10031.14.2017.711
31.11.11	10031.11.2017.0713
30.20.3.10012	10030.100.2017.0711
30.9.3	10030.100.2017.0713
30.6.7	10030.100.2017.0713

Cisco WebEx デスクトップアプリケーション バージョン アップの検証

シスコは次の製品で使用する Cisco WebEx デスクトップ アプリケーションのすべてのメジャー バージョンに対する修正をリリースしました。

- Cisco WebEx Meeting Center
- Cisco WebEx Event Center
- Cisco WebEx Training Center
- Cisco WebEx Support Center
- Cisco WebEx Meetings

Cisco WebEx Major Version	Fixed Desktop Application Version
WBS32	32.3.4.5
WBS31	31.14.3, 31.11.11
WBS30	30.20.3, 30.9.3, 30.6.7

注: WBS29 で利用可能な修正はありません。

現在の WebEx 顧客はサイトが WebEx ページことをの **サポート セクション**の **アプリケーション バージョン** 情報の確認によって更新済ソフトウェアを受け取ったことを確認できます。 この情報を表示するには、次の手順を実行します。

1. WebEx アカウントにサインインします
2. [Meeting Center] タブをクリックします。
3. [（Support）] [（Support）] 配下 [（Download）]
4. [Meeting Center について（About Meeting Center）] という見出しの下の画面の右側に、[アプリバージョン（Application Version）] が表示されます。

更新プログラムを自動受信していない場合、シスコ サポートまたはシスコ パートナーにお問い合わせください。

注: 導入済みサイトのアプリケーション バージョンとの互換性を確保するために、Cisco WebEx 製品のすべてのライセンス済み機能に対するクライアントをアップグレードする必要があります。 1 つのクライアントをアップグレードすることで、CVE-2017-6753 で文書化された脆弱性が解

決されます。 次のクライアントを使用できます。

- Cisco WebEx Meeting Center クライアント
- Cisco WebEx Event Center クライアント
- Cisco WebEx Training Center クライアント
- Cisco WebEx Support Center クライアント
- Cisco WebEx Access Anywhere クライアント
- Cisco WebEx Remote Access クライアント

Cisco WebEx Meetings

シスコは Cisco WebEx Meetings に対する修正をリリースしました。 Cisco WebEx Meetings ソフトウェアは T30.20.3 にアップグレードされました。

Cisco WebEx Meetings Server

Cisco WebEx Meetings サーバを展開した顧客は https://software.cisco.com/download/navigator.html?mdfid=282628019&flowid=76922 で、オンサイト Cisco WebEx サービス、更新済ソフトウェアをダウンロードするか、または Cisco Software Center から次のオプションを選択できます:
製品 > 会議ソリューション > Web 会議 > WebEx Meetings サーバ

Cisco WebEx Meetings Server バージョン 2.6 をお使いの場合は、Cisco WebEx Meetings Server バージョン 2.7 以降にアップグレードすることをお勧めします。 Cisco WebEx Meetings Server の次のリリースではこの脆弱性に対処するための更新が済んでいます。

- WebEx Meetings Server 2.6MR3 パッチ 5
- WebEx Meetings Server 2.7MR2 パッチ 9
- WebEx Meetings Server 2.8 パッチ 3

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

この脆弱性は、Google Project Zero の Tavis Ormandy 氏および Divergent Security の Cris Neckar 氏によってシスコに報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170717-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す。	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