Cisco WebEx Meetings Playerの任意のコード実行の脆弱性

Critical

アドバイザリーID : cisco-sa-20160831-meetings-player

初公開日 : 2016-08-31 16:00

最終更新日 : 2016-10-25 15:16

バージョン 1.2 : Final

CVSSスコア : 9.3

回避策 : No workarounds available

Cisco バグ ID : CSCva09375

CVE-2016-1464

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 Playerの脆弱性により、認証されていないリモートの攻撃者が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、ユーザが指定したファイルの不適切な処理に起因します。攻撃者は、該当ソフトウェアを使用して悪意のあるWRFファイルを開くようにユーザを誘導することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はユーザの権限を使用してシステム上で任意のコードを実行でき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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player

該当製品

脆弱性のある製品

この脆弱性は、Cisco WebEx Meetings Playerに影響します。修正済みリリースの詳細については、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

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

この脆弱性に対処する回避策はありません。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート（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 Technical Assistance Center（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/c/ja_jp/support/web/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。

修正済みソフトウェア

次の表では、左の列にCisco WebEx Meetingsソフトウェアのメジャーリリースを示します。右の列は、この脆弱性に対する修正を含む最初のリリースを示しています。

Cisco WebEx Meetingsメジャーリリース	First Fixed Release (修正された最初のリリース)
T31R2	T31R2以降
T31	T31.5.20以降
T30	T30.12.1以降
T29	T29.13.112以降

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。

出典

この脆弱性は、Francis Provencher(COSIG)によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	「malicious file」を「malicious WRF file」に変更。	要約	Final	2016年10月25日
1.1	修正済みソフトウェアリリースの表を追加。「脆弱性が存在する製品」セクションを「修正済みソフトウェア」セクションの新しい表を参照するように更新。	「該当製品」、「修正済みソフトウェア」	Final	2016年10月22日
1.0	初回公開リリース	-	Final	2016年8月31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。