Cisco WebEx Recording Format および Advanced Recording Format 対応のプレーヤーにおける複数の脆弱性

Critical

アドバイザリーID : cisco-sa-20171129-webex-players

初公開日 : 2017-11-29 16:00

最終更新日 : 2017-12-12 01:12

バージョン 1.4 : Final

CVSSスコア : 9.6

回避策 : No workarounds available

Cisco バグ ID : CSCve30268 CSCve10658 CSCve11507 CSCvf38077 CSCvf57234 CSCvg54843 CSCvf49707 CSCvg54868 CSCvg54867 CSCve11545 CSCvg54861 CSCve11548 CSCve30208 CSCve11503 CSCve10591 CSCve11538 CSCve10749 CSCve30214 CSCvg54836 CSCve10584 CSCvf38084 CSCve10762 CSCve11532 CSCvg54856 CSCve10764 CSCvg54850 CSCvg54853 CSCve10744 CSCvf38060 CSCvf49697 CSCvg54870 CSCvf49650 CSCve02843

CVE-2017-12368 CVE-2017-12369 CVE-2017-12367 CVE-2017-12371 CVE-2017-12372 CVE-2017-12370

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 ネットワーク録画プレーヤー（Advanced Recording Format（ARF）ファイルおよび WebEx Recording Format（WRF）ファイル対応）では、複数の脆弱性が存在します。 リモートの攻撃者はこれらの脆弱性をエクスプロイトすることで、電子メールまたは URL を通じて悪意のある ARF ファイルや WRF ファイルをユーザに与え、ファイルを起動するよう誘導する可能性

があります。 この脆弱性のエクスプロイトにより該当プレーヤーがクラッシュし、場合によってはターゲット ユーザのシステムで任意のコードを実行される危険性があります。

Cisco WebEx プレーヤーは、オンライン会議の出席者が録音した WebEx ミーティングのレコーディングを再生するためのアプリケーションです。 このプレーヤーは、ユーザが WebEx サーバ上でホストされる録画ファイルにアクセスするときに自動的にインストールされる場合があります。

シスコは、影響を受けるバージョンの Cisco WebEx Business Suite ミーティング サイト、Cisco WebEx Meetings サイト、Cisco WebEx Meetings Server、Cisco WebEx ARF Player および WRF Player を更新し、これらの脆弱性に対処しました。 これら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-20171129-webex-players

該当製品

脆弱性のある製品

本アドバイザリで公開されている脆弱性の影響を受けるものは、Cisco WebEx ARF Player および Cisco WebEx WRF Player です。 以下に示す Cisco WebEx Business Suite（WBS30、WBS31、WBS32）、Cisco WebEx Meetings のクライアント ビルド、Cisco WebEx Meetings Server が、本アドバイザリに記載の脆弱性のうち少なくとも 1 つの影響を受けます。

- Cisco WebEx Business Suite（WBS30）クライアント ビルド T30.20 より前
- Cisco WebEx Business SuiteWBS31 T31.20 前
- Cisco WebEx Business SuiteWBS32 T32.7 前
- Cisco WebEx Meetings T32.7 前）
- Cisco WebEx Meeting Server ビルド 2.7MR3 より前

Cisco WebEx ミーティング サイトで該当バージョンの WebEx クライアント ビルドを実行しているかどうかを判別するには、使用している Cisco WebEx ミーティング サイトにログインして、[サポート（Support）] > [ダウンロード（Downloads）] セクションに移動します。 WebEx クライアント ビルドのバージョンがページ右側の [Meeting Center について（About Meeting Center）] の下に表示されます。 詳細については、「修正済みソフトウェア」のセクションを参照してください。

また、Cisco WebEx ミーティング クライアントのバージョン情報には、Cisco WebEx ミーティング クライアント内からアクセスすることもできます。 Windows および Linux プラットフォームの Cisco WebEx ミーティング クライアントのバージョン情報は、[ヘルプ（Help）] > [Cisco WebEx Meeting Center について（About Cisco WebEx Meeting Center）] を選択することにより表示できます。 Mac プラットフォームの Cisco WebEx ミーティング クライアントの

バージョン情報は、[Meeting Center] > [Cisco WebEx Meeting Center について（About Cisco WebEx Meeting Center）] を選択することにより表示できます。

Cisco WebEx ソフトウェア アップデートは、クライアント ビルドの累積更新プログラムです。 たとえば、クライアント ビルド 30.32.16 が修正された場合、更新されたプログラムがビルド 30.32.17 に組み込まれます。 Cisco WebEx サイト管理者はセカンダリ バージョン名にアクセスできます。たとえば、T30 SP32 EP 16 はサーバが、クライアント ビルド 30.32.16 を実行していることを示します。

注: 自動ソフトウェア アップデートが受信されないお客様は、ソフトウェア メンテナンス終了に達したバージョンの Cisco WebEx を実行している可能性があります。該当する方はカスタマー サポートにお問い合わせください。

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。

詳細

Cisco WebEx Business Suite（WBS）会議サービスおよび Cisco WebEx Meetings は、Cisco WebEx が管理保守するホステッド マルチメディア会議ソリューションです。 Cisco WebEx Meetings Server はお客様のプライベート クラウドでホスト可能なマルチメディア会議ソリューションです。

ARF および WRF ファイル形式を使用して、WebEx 会議サイト、またはオンライン会議出席者のコンピュータ上に記録されている WebEx 会議の録画を保存します。

Cisco WebEx ARF Player および Cisco WebEx WRF Player は、WebEx ARF および WRF 録画ファイル（拡張子が .arf、.wrf のファイル）の再生、編集のためのアプリケーションです。

Cisco WebEx ARF Player および Cisco WebEx WRF Player は、WebEx ミーティング サイトでホストされる録画ファイルに（ストリーミング再生モードで）アクセスすると自動的にインストールされる場合があります。 、Cisco WebEx ARF Player Cisco WebEx WRF Player http://www.webex.com/play-webex-recording.html

Cisco WebEx ARF Player は、Cisco WebEx ミーティング サイト クライアント（WBS30、WBS31、WBS32、Cisco WebEx Meetings）、Cisco WebEx Meetings Server クライアントのすべてで利用できます。 Cisco WebEx WRF Player は、Cisco WebEx ミーティング サイト クライアント（WBS30、WBS31、WBS32）でのみ利用でき、Cisco WebEx Meetings または Cisco WebEx Meetings Server クライアントでは利用できません。

次の表に、本アドバイザリに記載の脆弱性に割り当てられた Cisco Bug ID および Common Vulnerabilities and Exposures（CVE）ID を示します。

タイトル	CVE ID	
Cisco WebEx ネットワーク録画プレーヤーにおける Denial of Service（DoS）の脆弱性	CVE-2017-12367	CSCve11545、CSCve02843、
Cisco WebEx ネットワーク録画プレーヤーにおける リモート コード実行の脆弱性	CVE-2017-12368	CSCve10584、CSCve10591、
Cisco WebEx ネットワーク録画プレーヤーにおける 境界外の脆弱性	CVE-2017-12369	CSCve30208、CSCve30214、
Cisco WebEx ネットワーク録画プレーヤーにおける リモート コード実行の脆弱性	CVE-2017-12370	CSCvf38060、CSCvg54836、
Cisco WebEx ネットワーク録画プレーヤーにおける リモート コード実行の脆弱性	CVE-2017-12371	CSCvf49650、CSCvg54853、
Cisco WebEx ネットワーク録画プレーヤーにおける リモート コード実行の脆弱性	CVE-2017-12372	CSCvf57234、CSCvg54868、

これらの脆弱性がエクスプロイトされると、プレーヤー アプリケーションがクラッシュしたり、リモートの攻撃者によって悪意のあるコードが実行される可能性があります。

これらの脆弱性をエクスプロイトするには、プレーヤー アプリケーションから悪意のある ARF ファイルや WRF ファイルを開く必要があります。 攻撃者は、悪意のある録画ファイルをユーザに直接（たとえば電子メールを使用して）提供するか、悪意のある Web ページに誘導することで、この脆弱性をエクスプロイトできる可能性があります。 ただし、WebEx ミーティングに参加しているユーザによってエクスプロイトされる危険性はありません。

回避策

これらの脆弱性に対処する回避策はありません。 、Meeting Services Removal Tool（Microsoft Windows Mac WebEx Meeting Application Uninstaller（Apple Mac OS X WebEx 、Cisco Spark、WebEx、Jabber 向 Cisco Collaboration Help 記事（https://collaborationhelp.cisco.com/article/en-us/WBX000026396） 。

Linux または UNIX ベース システムの WebEx ソフトウェアは、Cisco Spark、WebEx、Jabber 向けの Cisco Collaboration Help の記事にある手順（以下の URL を参照）にしたがって削除することができます。 https://collaborationhelp.cisco.com/article/en-us/WBX28548

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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

以下に示す Cisco WebEx Business Suite（WBS30、WBS31、WBS32）、Cisco WebEx Meetings のクライアント ビルド、および Cisco WebEx Meetings Server は、本アドバイザリに記載の脆弱性すべてに対処しています。

- Cisco WebEx Business Suite（WBS30）クライアント ビルド T30.20 以降
- Cisco WebEx Business Suite（WBS31）クライアント ビルド T31.20 以降
- Cisco WebEx Business Suite（WBS32）クライアント ビルド T32.7 以降
- Cisco WebEx Meetings（クライアント ビルド T32.7 以降）
- Cisco WebEx Meeting Server ビルド 2.7MR3 以降、2.8MR1 以降、3.0 以降

Cisco WebEx ミーティング サイトで該当バージョンの WebEx クライアント ビルドを実行しているかどうかを判別するには、使用している Cisco WebEx ミーティング サイトにログインして、[サポート（Support）] > [ダウンロード（Downloads）] セクションに移動します。 WebEx ク

ライアント ビルドのバージョンがページ右側の [Meeting Center について (About Meeting Center)] の下に表示されます。 Cisco WebEx ソフトウェア アップデートは、クライアント ビルドの累積更新プログラムです。 たとえば、クライアント ビルド 30.32.16 が修正された場合、更新されたプログラムがビルド 30.32.17 に組み込まれます。

本アドバイザリで公開されている脆弱性の影響を受けるものは、Cisco WebEx ARF Player と Cisco WebEx WRF Player です。 Microsoft Windows、Apple Mac OS X、Linux バージョンのプレーヤーはすべて、本アドバイザリに記載の脆弱性のうち少なくとも 1 つの影響を受けます。 Cisco WebEx ARF Player または Cisco WebEx WRF Player が自動でインストールされている場合は、WebEx ミーティング サイト上でホストされている録画ファイルにアクセスした際に、脆弱性のない最新のバージョンに自動的にアップグレードされます。 Cisco WebEx ARF Player Cisco WebEx WRF Player 、http://www.webex.com/play-webex-recording.html

インストールされている Cisco WebEx ARF Player または Cisco WebEx WRF Player のバージョンを自身で確認し、これらの脆弱性の影響を受けるかどうかを判断できます。

注: お持ちの WebEx Business Suite がロックダウン状態にあるお客様が WebEx サイトに該当するパッチを適用する場合は、WebEx サポートにお問い合わせください。

Cisco Bug ID	First Fixed Release (修正された最初のリリース)				
	WBS30	WBS31	WBS32	WebEx Meetings	WebEx Meetings Serve
CSCve11545					2.7MR3 2.8MR1
CSCve02843	T30.20	T31.14	T32.2		
CSCve11548				T30.20 T32.2	
CSCve10584		T31.14.4 T31.15	T32.3		
CSCve10591					2.7MR3 2.8MR1
CSCve11503				T32.3	
CSCve10658		T31.14.4	T32.4		
CSCve11507				T32.3	
CSCve10749					2.7MR3 2.8MR1
CSCve10744		T31.14.4	T32.2		
CSCve11532				T32.2	
CSCve10762			T32.4		
CSCve10764					3.0
CSCve11538				T32.2	
CSCve30208		T31.14.4 T31.15 T31.17.2	T32.3 T32.6		
CSCve30214					2.7MR3 2.8MR1
CSCve30268				T32.4	

				T32.6	
CSCvf38060		T31.17	T32.5		
CSCvg54836				T32.7	
CSCvf38077		T31.17	T32.5		
CSCvg54843				T32.7	
CSCvf38084		T31.17	T32.5		
CSCvg54850				T32.7	
CSCvf49650		T31.20	T32.6		
CSCvg54853					3.0
CSCvg54856				T32.7	
CSCvf49697		T31.20	T32.6		
CSCvg54861				T32.7	
CSCvf49707		T31.20	T32.7		
CSCvg54867				T32.7	
CSCvf57234		T31.17.2	T32.6		
CSCvg54868					3.0
CSCvg54870				T32.7	

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

これらの脆弱性は、以下のとおり Yihan Lian、Fortinet、Trend Micro によって報告されました。

Cisco Bug ID
CSCve11545、CSCve02843、CSCve11548、CSCve30208、CSCve30214、CSCve30268
CSCve10584、CSCve10591、CSCve11503、CSCve10658、CSCve11507、CSCve10749、CSCve107
CSCvf38077、CSCvg54843、CSCvf38060、CSCvg54836、CSCvf38084、CSCvg54850、CSCvf49650
CSCvf57234、CSCvg54868、CSCvg54870

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-webex-players

改訂履歴

Version	Description	Section	Status	日付
1.4	明記。	該当製品	Final	2017 年 12 月 12 日
1.3	当初の修正バージョンに関して説明を明記。	修正済みソフトウェア	Final	2017 年 11 月 30 日
1.2	「出典」セクションで研究者の情報を更新。	Source	Final	2017 年 11 月 30 日
1.1	CVE-2017-12370「詳細」セクションに記載のバグ ID を訂正。	Details	Final	2017 年 11 月 29 日
1.0	初回公開リリース		Final	2017 年 11 月 29 日

利用規約