Cisco WebEx Network Recording Player Multiple Buffer Overflow Vulnerabilities

High

アドバイザリーID : cisco-sa-20170621-wnrp

初公開日 : 2017-06-21 16:00

最終更新日 : 2017-06-26 15:12

バージョン 1.1 : Final

CVSSスコア : 7.3

回避策 : No workarounds available

Cisco バグ ID : CSCvc51227 CSCvc47758 CSCvc51242

CVE-2017-6669

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 Network Recording Player の Advanced Recording Format (ARF) ファイルに、複数のバッファ オーバーフロー脆弱性が存在します。 攻撃者はこ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 Network Recording Player は、オンライン会議参加者のコンピュータに記録された WebEx ミーティング録画の再生に使用される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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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。
621-wnrp

該当製品

脆弱性のある製品

この脆弱性は Cisco WebEx ARF Player に影響を与えます。 次のクライアント ビルドが、この脆弱性に該当します。

- T29.13.130 より前の Cisco WebEx Business Suite（WBS29）クライアント ビルド
- T30.17 より前の Cisco WebEx Business Suite（WBS30）クライアント ビルド
- T31.10 より前の Cisco WebEx Business Suite（WBS31）クライアント ビルド

、ユーザは Cisco WebEx 会議サイトにログイン Cisco WebEx 会議サイトが WebEx クライアント ビルドの影響を受けたバージョンを実行しているかどうか判別し、 **サポート > ダウンロード** セクションに行くためにできます。 WebEx クライアントのバージョンがページ右側の [Support Center について（About Support Center）] の下に表示されます。

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 会合クライアントのためのバージョン情報は **Cisco WebEx Meeting Center を** Help > About の順に選択 することによって表示することができます。 Mac プラットフォームの Cisco WebEx 会議クライアントのためのバージョン情報は **Cisco WebEx Meeting Center についての会議センターの >** 選択によって表示することができます。

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 29.32.16 が修正された場合、更新されたプログラムがビルド 29.32.17 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、T29 SP32 EP16 はサーバが、クライアント ビルド 29.32.16 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。

シスコは、この脆弱性が Cisco WebEx WRF Player には影響を与えないことを確認しました。

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、会合サービス取り外しツール（Microsoft ウィンドウ ユーザ向けに）または DOC-2672 で利用可能 な Mac Cisco WebEx アンインストーラを使用してシステムからすべての WebEx ソフトウェアを（Apple Mac OS X ユーザ向けに）完全に取除くことは可能性のあるです。

Linux または UNIX ベースのシステムから WebEx ソフトウェアを削除するには、次のリンクの WebEx ナレッジ ベースの記事の手順に従ってください。
https://support.webex.com/MyAccountWeb/knowledgeBase.do?root=Tools&parent=Knowledge&articleId=WBX28548&txtSearchQuery=uninstall%20linux#。

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

Cisco WebEx Business Suite（WBS29、WBS30、WBS31）の以下のクライアントはこの脆弱性に対応しています。

- T29.13.130 以降の Cisco WebEx Business Suite（WBS29）クライアント ビルド
- T30.17 以降の Cisco WebEx Business Suite（WBS30）クライアント ビルド
- T31.10 以降の Cisco WebEx Business Suite（WBS31）クライアント ビルド

、ユーザは Cisco WebEx 会議サイトにログイン Cisco WebEx 会議サイトが WebEx クライアント ビルドの影響を受けたバージョンを実行しているかどうか判別し、 **サポート > ダウンロード** セクションに行くためにできます。 WebEx クライアントのバージョンがページ右側の [Support Center について（About Support 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 29.32.16 が修正された場合、更新されたプログラムがビルド 29.32.17 に組み込まれます。

WebEx サイトから ARF プレイヤーを直接ダウンロードしたユーザは http://www.webex.com/play-webex-recording.html からアプリケーションをダウンロードすることによってプレイヤーを手動でアップデートできます。

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。

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、Trend Micro の Zero Day Initiative に参加している Source Incite の Steven Seeley 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-20170621-wnrp

改訂履歴

Version	Description	Section	Status	日付
1.1	Corrected the source information.	Source	Final	2017-June-26
1.0	Initial public release.		Final	2017-June-21

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。