Cisco WebEx ネットワーク レコード プレーヤ バッファオーバーフローの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20180103-wnrp **初公開日 :** 2018-01-03 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.5 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg78839 CSCvg78837 CSCvg78835	CVE-2018-0103

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

高度レコード形式（ARF）ファイルのための Cisco WebEx ネットワーク レコード プレーヤの脆弱性はローカル攻撃者がユーザのシステムの任意のコードを実行することを可能にする可能性があります。 攻撃者はユーザを悪意のある ARF ファイルのリンクか電子メールの添付ファイル 送信 し、ユーザをリンクに従うか、またはファイルを開くように説得することによってこの脆弱性を不正利用する可能性があります。 不正利用の成功は攻撃者がユーザのシステムの任意のコードを実行することを可能にする可能性があります。

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。

Cisco はこの脆弱性に対処するために Cisco WebEx ビジネス スイート会議サイト、Cisco WebEx Meetings サイト、Cisco WebEx Meetings サーバおよび Cisco WebEx ARF プレイヤーの影響を受けたバージョンをアップデートしました。

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。
103-wnrp

該当製品

脆弱性のある製品

この脆弱性は Cisco WebEx ビジネス スイート会議サイト、Cisco WebEx Meetings サイト、Cisco WebEx Meetings サーバおよび Cisco WebEx ARF プレイヤーに影響を与えます。 該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。 ただし、会合サービス取り外しツール（Microsoft ウィンドウのために）または Mac WebEx 会合アプリケーション アンインストーラ（Apple Mac OS X のために）、Cisco Spark、WebEx および https://collaborationhelp.cisco.com/article/en-us/WBX000026396 で Jabber 記事のための Cisco コラボレーション ヘルプからのダウンロードのための利用可能 なを使用してシステムからすべての WebEx ソフトウェアを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の WebEx ソフトウェアの削除は https://collaborationhelp.cisco.com/article/en-us/WBX28548 の Cisco Spark、WebEx および Jabber 技術情報のための Cisco コラボレーション ヘルプのステップに従うことによって達成することができます。

修正済みソフトウェア

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。

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

Cisco はトレンドマイクロのゼロ日コントロールを使用しているこの脆弱性を報告するために攻撃的なセキュリティのスティーブン Seeley に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180103-wnrp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-January-03

利用規約