Cisco WebEx Recording Format Playerの情報漏えいの脆弱性

Medium

アドバイザリーID : cisco-sa-20180502-webex-id
初公開日 : 2018-05-02 16:00
最終更新日 : 2018-05-08 16:31
バージョン 1.1 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCvh89113 CSCvh89132 CSCvh89142 CSCvh89107

CVE-2018-0288

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 Recording Format(WRF)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アプリケーションに関する機密データにアクセスできる可能性があります。攻撃者は、この脆弱性を不正利用して情報を取得し、さらなる偵察攻撃を実行する可能性があります。

この脆弱性は、Cisco WRF Playerの設計上の欠陥に起因します。攻撃者は、悪意をもって巧妙に細工されたファイルを利用することで、この脆弱性を不正利用し、コード内のチェックをバイパスして、マッピングファイルの範囲外からメモリを読み取る可能性があります。

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-20180502-webex-id

該当製品

脆弱性のある製品

この脆弱性は、Cisco WebEx Business Suite会議サイト、Cisco WebEx Meetingsサイト、およびCisco WebEx WRFプレーヤーに影響を与えます。該当するソフトウェアリリースの詳細については、このアドバイザリの冒頭にあるCisco Bug IDを参照してください。

Cisco WebEx Meetingsサイトで該当バージョンのWebExクライアントビルドが実行されてい

るかどうかを確認するには、Cisco WebEx Meetingsサイトにログインして、Support > Downloadsの順に選択します。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。

また、Cisco WebEx Meetingsクライアント内からCisco WebEx Meetingsクライアントのバージョン情報にアクセスすることもできます。WindowsおよびLinuxプラットフォーム上のCisco WebEx Meetingsクライアントのバージョン情報を表示するには、Help > About Cisco WebEx Meeting Centerの順に選択します。Macプラットフォーム上のCisco WebEx Meetingsクライアントのバージョン情報を表示するには、Meeting Center > About Cisco WebEx Meeting Centerの順に選択します。

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を受け取らないお客様は、ソフトウェアメンテナンスが終了したバージョンのCisco WebExを実行している可能性があるため、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

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

詳細

Cisco WebEx Business Suite（WBS）会議サービスは、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。

WRFファイル形式は、WebEx会議サイトに記録されたWebEx会議の記録を保存するために使用されます。

Cisco WebEx WRF Playerは、WebEx WRF録画ファイル(.wrf拡張子の付いたファイル)の再生と編集に使用するアプリケーションです。

Cisco WebEx WRF Playerは、Cisco WebEx Meetingsサイトでホストされている録画ファイルにアクセスすると自動的にインストールされます（ストリーム再生モード用）。Cisco WebEx WRF Player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して手動でインストールし、録画ファイルをオフラインで再生することもできます。

Cisco WebEx WRF Playerは、すべてのCisco WebEx Business Suiteクライアント（WBS31およびWBS32）とCisco WebEx Meetingsクライアントで使用できます。

このアドバイザリで説明されている脆弱性により、攻撃者はコード内のチェックをバイパスし、マッピングファイルの範囲外からメモリを読み取る可能性があります。

この脆弱性を不正利用するには、プレーヤーアプリケーションで悪意のあるWRFファイルを開く必要があります。この脆弱性は、WebEx会議に参加しているユーザによって引き起こされることはありません。

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、Meeting Services Removal Tool（Microsoft Windowsの場合）またはMac WebEx Meeting Application Uninstaller（Apple Mac OS Xの場合）を使用して、システムからすべてのCisco WebExソフトウェアを完全に削除することができます。どちらのツールも、https://collaborationhelp.cisco.com/article/en-us/WBX000026396のCisco Spark、WebEx、およびJabberのCisco Collaborationヘルプの記事からダウンロードできます。

LinuxまたはUNIXベースのシステムからのCisco WebExソフトウェアの削除は、https://collaborationhelp.cisco.com/article/en-us/WBX28548にあるCisco Spark、WebEx、およびJabber向けのCisco Collaborationヘルプの記事の手順に従って行うことができます。

修正済みソフトウェア

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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。

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、Trend MicroのZero Day Initiativeに協力している匿名の報告者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-20180502-webex-id

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	ソース情報を更新。	出典	Final	2018 年 5 月 8 日
1.0	初回公開リリース	—	Final	2018 年 5 月 2 日

利用規約

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。