Cisco Webex Playerのメモリ破損の脆弱性

High

アドバイザリーID : cisco-sa-webex-player-kOf8zVT

CVE-2021-1526

初公開日 : 2021-06-02 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCvx58407

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 Player for Windows and MacOSの脆弱性により、攻撃者は該当システムで任意のコードを実行できる可能性があります。

この脆弱性は、Webex Recording Format(WRF)のWebexレコーディングファイルの値の検証が不十分であることに起因します。 攻撃者は、悪意のあるWRFファイルをリンクまたは電子メールの添付ファイルを通じてユーザに送信し、ローカルシステム上の該当ソフトウェアでファイルを開くようにユーザに促すことで、この脆弱性を不正利用する可能性があります。不正利用が成功すると、攻撃者はターゲット ユーザの権限を使用して、影響を受けるシステムで任意のコードを実行す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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-kOf8zVT

該当製品

脆弱性のある製品

この脆弱性は、リリース41.5より前のCisco Webex Player for WindowsおよびMacOSリリースに影響を与えます。このプレーヤーは、Cisco Webex Meetingsサイトから入手できます。

システムにインストールされているCisco Webex Playerのリリースを確認するには、プレーヤーを開き、[ヘルプ] > [バージョン情報]を選択します。

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。

Cisco Webex Network Recording Player for Windows and MacOSは、この脆弱性の影響を受けません。

詳細

Cisco Webex Meetings は、Cisco Webex によって管理保守され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 サーバは、お客様のプライベート クラウドでホストおよび管理保守するマルチメディア会議ソリューションです。

Cisco Webex Meetings サービスは、ユーザが会議記録をオンラインで保存し、ARF ファイルとしてダウンロードできるように設定できます。これらのサービスは、ユーザのローカル コンピュータに WRF ファイルとして、会議を直接録音するように設定することもできます。

Cisco Webex ネットワーク録画プレーヤーは、ARF ファイルの再生に使用されます。Cisco Webex Meetings サイトと Cisco Webex Meetings サーバから入手できます。このプレーヤーは、ユーザのCisco Webex Webサイトのダウンロードページからクラシック表示で手動でインストールするか、Cisco Webexビデオ録画ページからインストールできます。

Cisco Webex プレーヤーは、WRF ファイルの再生に使用されます。Cisco Webex Meetings サイトから入手できます。Cisco WebEx Meetings サーバからは入手できません。このプレーヤーは、ユーザのCisco Webex Webサイトのダウンロードページからクラシック表示で手動でインストールするか、Cisco Webexビデオ録画ページからインストールできます。

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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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 Cisco Service Contract 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 POS 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。
https://www.cisco.com/c/en/us/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。

修正済みリリース

シスコは、Cisco Webex Playerリリース41.5以降でこの脆弱性を修正しました。リリースは、Cisco Webex Video Recordingページまたは対応するCisco Webex Meetingsサイトから入手できます。

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

この脆弱性を報告していただいたFortinet社のKushal Arvind Shah氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-kOf8zVT

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	最終版	2021 年 6 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。