Cisco Security Advisory: Buffer Overflow Vulnerabilities in the Cisco WebEx Player

Advisory ID: cisco-sa-20111026-webex

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-webex

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。

Revision 1.0

For Public Release 2011 October 26 16:00 UTC (GMT)

目次

要約

Cisco WebEx Recording Format (WRF) Player に、バッファ オーバーフローを引き起こす脆弱性が複数存在します。この脆弱性を不正利用することで、攻撃者はリモートから、対象ユーザの権限によってシステムで任意のコードを実行することが可能になる場合があります。

Cisco WebEx Player は、WebEx 会議サイトで記録された、また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 会議を再生するアプリケーションです。これらのプレーヤーは、ユーザが WebEx 会議サイトにあるレコーディング ファイルにアクセスすると自動でインストールされます。または、オフラインで再生する場合、www.webex.com からアプリケーションをダウンロードし、手動でインストールすることもできます。

WRF プレーヤーを自動でインストールした場合は、WebEx 会議サイトにあるレコーディング ファイルにアクセスすることで、脆弱性のない最新バージョンへと自動でアップグレードされます。WRF プレーヤーを手動でインストールした場合は、www.webex.com から最新バージョンをダウンロードして、手動で新しいバージョンのプレーヤーをインストールする必要があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。

このアドバイザリは次のリンクに掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-webex

注：2011 年 10 月 18 日に、シスコは Cisco PSIRT により公開された現行の Cisco Security Advisories and Responses の一覧の場所を移動しました。新しい場所は次のとおりです。
http://tools.cisco.com/security/center/publicationListing
Cisco Security Intelligence Operations（SIO）ポータルの [Cisco Products and Services] メニューからもこのページに移動することができます。この移行後、新しい Cisco Security Advisories and Responses はこの新しい場所で公開されます。URL は変更されましたが、セキュリティ ドキュメントと脆弱性ポリシーの内容に変更はありません。シスコは公開された Security Vulnerability Policy（セキュリティ脆弱性ポリシー）にしたがってセキュリティ脆弱性の開示を続けます。

該当製品

このアドバイザリで公開される脆弱性は、Cisco WRF Player に影響を与えます。Microsoft Windows、Apple Mac OS X、Linux に対応するバージョンのプレーヤーはすべて影響を受けます。脆弱性のないコードを含むリリースの一覧を次の表に示します。該当するプレーヤーのバージョンは、クライアント ビルド T26 SP49 EP40 および T27 SP28 よりも前のバージョンです。これらのビルド 番号は WebEx サイト管理者にのみ表示されます。エンド ユーザには「Client build: 27.25.4.11889」などのバージョンが表示されます。これはサーバがソフトウェア バージョン T27 SP25 EP4 を実行していることを示します。

Cisco WebEx 会議サイトで該当するバージョンの 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、ご利用の Cisco WebEx 会議サイトにログインして、[サポート] から [ダウンロード] セクションに進みます。WebEx クライアント ビルドのバージョンは、ページ右にある [サポート センターについて] の下に表示されています。詳細は、「ソフトウェア バージョンおよび修正」を参照してください。

シスコでは、最新バージョンのプレーヤーへアップグレードすることを推奨しています。www.webex.com/downloadplayer.html で入手できます。プレーヤーが不要になった場合は、support.webex.com/support/downloads.html にある Mac Cisco-WebEx Uninstaller または Meeting Services Removal Tool を利用して削除できます。

インストールされた WRF プレーヤーのバージョンを手動で確認し、これらの脆弱性による影響を受けるかどうかについて判断することができます。これを行うには、管理者がインストールされたファイルのバージョンを確認し、ファイルのバージョンが修正済みのコードを含むかどうかを確認する必要があります。バージョン番号の確認方法に関する詳細な説明は、次のセクションに記載されています。

次のテーブルには、各オブジェクトの脆弱性がない最初のバージョンが記載されています。
Microsoft Windows

脆弱性が存在する製品

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。

脆弱性が存在しない製品

WebEx Advanced Recording Format（ARF）用 Cisco WebEx Player は、このアドバイザリで説明されている脆弱性の影響を受けません。

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

WebEx 会議サービスは、Cisco Web Ex が管理および保守するホスト型の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、またはオンライン会議の参加者のコンピュータに記録された WebEx 会議のレコーディング内容を保存するために使用されます。プレーヤーは、レコーディング ファイル（*.wrf* の拡張子が付いたファイル）を再生および編集するためのアプリケーションです。WRF プレーヤーは、ユーザが WebEx 会議サイトにあるレコーディング ファイルにアクセスすると自動でインストールされます（ストリーミング再生時）。また、レコーディング ファイルをローカルで再生する場合（オフライン再生時）、www.webex.com/downloadplayer.html からアプリケーションをダウンロードし、手動でインストールすることもできます。

Cisco WebEx Recording Format（WRF）Player は、次の脆弱性の影響を受けます。

Cisco WebEx Player WRF 解析の脆弱性
この脆弱性には Common Vulnerabilities and Exposures（CVE）ID として CVE-2011-3319 が割り当てられています。

Cisco WebEx Player ATAS32 処理の脆弱性
この脆弱性には Common Vulnerabilities and Exposures（CVE）ID として CVE-2011-4004 が割り当てられています。

これらの脆弱性によって、プレーヤー アプリケーションがクラッシュする可能性があるほか、場合によってはリモートからコードが実行される恐れもあります。

これら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不正な WRF ファイルを開く必要があります。攻撃者は、ユーザに不正なレコーディング ファイルを直接提供する（電子メールを利用するなど）か、ユーザを不正な Web ページへ移動させることで不正アクセスを試みます。WebEx 会議に参加しているユーザによってこれらの脆弱性が引き起こされることはありません。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次の URL にて CVSS に関する FAQ を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

Multiple Cisco WebEx Player Buffer Overflow Vulnerabilities Calculate the environmental score of these					
CVSS Base Score - **9.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **7.7**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このドキュメントで説明されている脆弱性が悪用されると、Cisco WRF プレーヤー アプリケーションがクラッシュする可能性があります。また、場合によっては、WRF プレーヤー アプリケーションを実行しているユーザの権限を使用して、リモートの攻撃者がシステムで任意のコードを実行できる可能性もあります。

ソフトウェア バージョンおよび修正

ソフトウェア アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリを参照して、問題の解決状況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。

これらの脆弱性は、次のバージョンから修正されています。

- T26 SP49 EP40
- T27 FR20
- T27 SP11 EP23
- T27 SP21 EP9
- T27 SP23
- T27 SP25 EP3
- T27 SP28

クライアント ビルドはご契約の Cisco WebEx サイトにログインし、[サポート] > [ダウンロード] セクションにてご確認いただけます。WebEx の不具合修正は、メジャー リリースに組み込まれます。たとえば、リリース T27 SP22 EP9 が修正されると、リリース T27 SP22 EP23 でもソフトウェア修正が行われます。エンド ユーザには「Client build: 27.25.4.11889」などのバージョンが表示されます。これはサーバがソフトウェア バージョン T27 SP25 EP4 を実行していることを示します。

WRF プレーヤーを自動でインストールした場合は、WebEx 会議サイトにあるレコーディング ファイルにアクセスすることで、脆弱性のない最新バージョンへと自動でアップグレードされます。

また、WRF プレーヤーを手動でインストールした場合は、www.webex.com/downloadplayer.html から最新バージョンをダウンロードして、手動で新しいバージョンのプレーヤーをインストールする必要があります。プレーヤーが不要になった場合は、support.webex.com/support/downloads.html にある Mac Cisco-WebEx Uninstaller または Meeting Services Removal Tool を利用して削除できます。

回避策

このアドバイザリに記載されている脆弱性に対する回避策はありません。

修正済みソフトウェアの入手

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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、ご購入いただいたフィーチャ セットに対してのみとなります。お客様はソフトウェア 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利用することにより、http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html または http://www.cisco.com/public/sw-center/sw-usingswc.shtml に記載されているシスコのソフトウェア ライセンス条件に同意したものと見なされます。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

このセクションは、Cisco WebEx 製品の脆弱性には適用されません。

サードパーティのサポート会社をご利用のお客様

このセクションは、Cisco WebEx 製品の脆弱性には適用されません。

サービス契約をご利用でないお客様

このセクションは、Cisco WebEx 製品の脆弱性には適用されません。

不正利用事例と公式発表

Cisco PSIRT では、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とその公表は確認しておりません。

これらの脆弱性は、TippingPoint 社からシスコに報告されたものです。TippingPoint 社に感謝いたします。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-webex

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-October-26	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは

http://www.cisco.com/go/psirt/ で確認することができます。