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

Advisory ID: cisco-sa-20120404-webex

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120404-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 2012 April 4 16:00 UTC (GMT)

目次

要約

Cisco WebEx Recording Format (WRF) Player には、バッファ オーバーフローを引き起こす脆弱性が 3 つ存在します。リモートの攻撃者はこの脆弱性を不正利用することで、対象ユーザの権限を使用してシステム上の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 会議サイトに記録された、あるいは、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、 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、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、該当バージョンの WebEx 会議サイトおよび WRF プレーヤーをアップデートし、上記の脆弱性に対応しています。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120404-webex

該当製品

脆弱性が存在する製品

このアドバイザリで公開される脆弱性は、Cisco WebEx Recording Format（WRF）Player に影響を与えます。Cisco WebEx Business Suite（WBS27）の以下に示すクライアント ビルドは、このアドバイザリで説明する脆弱性のうち、少なくとも 1 つの脆弱性の影響を受けます。

- クライアント ビルド 27.32.0（T27 LD SP32）以前
- クライアント ビルド 27.25.9（T27 LC SP25 EP9）以前
- クライアント ビルド 27.21.10（T27 LB SP21 EP10）以前
- クライアント ビルド 27.11.26（T27 L SP11 EP26）以前

WebEx のクライアント ビルドを確認するには、ご利用の 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] セクションに進んでください。ページの右側に WebEx クライアント ビルドのバージョンが表示されます。Cisco WebEx のソフトウェア アップデートは、クライアント ビルドに累積されます。たとえば、クライアント ビルド 27.32.10 が修正された場合、そのソフトウェア アップデートはビルド 27.32.11 に含まれることになります。Cisco WebEx サイト管理者は、2 番目のバージョン名（T27 SP25 EP10 など）を使用することができます。たとえば、T27 SP25 EP10 の場合、サーバーでクライアント ビルド 27.25.10 が稼働していることを示します。

注：ソフトウェア アップデートが自動で受信されない場合、ソフトウェア メンテナンスが終了しているバージョンの Cisco WebEx が稼働している可能性があります。

脆弱性が存在しない製品

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。

WBS28 には、このアドバイザリで説明する脆弱性は存在しません。

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）。 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することにより、ローカルでレコーディング ファイルを再生することもできます（オフライン再生時）。

このアドバイザリで説明するバッファ オーバーフローに関する脆弱性に対しては、次の

Common Vulnerabilities and Exposures（CVE）ID 番号が割り当てられています。

- CVE-2012-1335
- CVE-2012-1336
- CVE-2012-1337

これらの脆弱性が不正利用されることによって、プレーヤー アプリケーションが破損したり、場合によってはリモートからコードが実行されたりする可能性があります。

これら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組織の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、自身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。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

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 計算ツールを次のリンクで提供しています。

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

Multiple Cisco WebEx Player Buffer Overflow Vulnerabilities Calculate the environmental score of					
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

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も参照して、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。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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。

下記の Cisco WebEx Business Suite（WBS27）では、このアドバイザリで説明される脆弱性は修正されています。

- クライアント ビルド 27.25.10（T27 LC SP25 EP10）
- クライアント ビルド 27.32.1（T27 LD SP32 CP1）

T27 SP25 より前のクライアント ビルドのサポートは終了しています。修正済みのソフトウェアを入手するには、最新バージョンにアップグレードしてください。

WebEx のクライアント ビルドを確認するには、ご利用の 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]** セクションに進んでください。ページの右側に WebEx のクライアント ビルドのバージョンが表示されます。Cisco WebEx のソフトウェア アップデートは、クライアント ビルドに累積されます。たとえば、クライアント ビルド 27.25.10 が修正された場合、そのソフトウェア アップデートはビルド 27.25.11 に含まれることになります。

Microsoft Windows、Apple Mac OS X、および Linux に対応するバージョンの Cisco WRF プレーヤーはすべて影響を受けます。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。Cisco WebEx プレーヤーを手動でインストールした場合は、http://www.webex.com/play-webex-recording.html から最新バージョンをダウンロードして、手動でインストールする必要があります。プレーヤーを完全に削除するには、http://support.webex.com/support/downloads.html にある Meeting Services Removal Tool または Mac Cisco-WebEx Uninstaller（Apple Mac ユーザの場合）にアクセスしてください。

プレーヤーがこれらの脆弱性の影響を受けるかどうかを判断するには、インストールしたバージョンを手動で確認します。その場合、ファイル バージョンを確認することで、そのバージョンに修正済みコードが存在しているかどうかを確認できます。

Microsoft Windows

Microsoft Windows プラットフォームでは、このアドバイザリで説明される脆弱性に対応するために、1 つのダイナミック リンク ライブラリ（DLL）がアップデートされています。それらのファイルは、C:¥Program Files¥WebEx¥Record Playback フォルダまたは C:¥Program Files (x86)¥Webex¥Record Player フォルダにあります。DLL のバージョン番号の確認は、Windows エクスプローラで Record Playback ディレクトリを開き、ファイル名を右クリックして [プロパテ

ィ] を選択します。[プロパティ] の [バージョン] または [詳細] タブにライブラリ バージョンの詳細が表示されています。以下の表には、DLL *atas32.dll* の最初の修正バージョンが記載されています。インストールされているバージョンが表に記載されたバージョンまたはそれ以降であれば、システムに脆弱性はありません。

クライアント ビルド	Cisco WRF DLL ファイル名	DLL ファイルのバージョン
27.25.10	atas32.dll	2.6.25.1
27.25.10	atdl2006.dll	1027.1125.1206.1310
27.32.1	atas32.dll	2.6.32.2

Apple Mac

Apple Mac OS プラットフォームでは、このアドバイザリで説明されている脆弱性に対応するために、3 つのパッケージ バンドルがアップデートされています。このファイルは、各ユーザのホーム ディレクトリにあり、~/Library/Application Support/WebEx Folder/924 からアクセスできます。バージョンの確認は、Finder で該当するフォルダを開き、ファイル名を Ctrl +クリックします。メニューが表示されたら、[**パッケージの内容を表示**] を選択し、*Info.plist* ファイルをダブルクリックします。表示されたテーブルの下部にバージョン番号が表示されます。以下の表には、各パッケージ バンドルの最初の修正バージョンが記載されています。インストールされているバージョンが表に記載されたバージョンまたはそれ以降であれば、システムに脆弱性はありません。

クライアント ビルド	Cisco WRF バンドル ファイル名	バンドル ファイルのバージョン
27.25.10	atas.bundle	12.15.25.3
27.32.1	atas.bundle	12.13.32.0
27.32.1	asplayback.bundle	12.13.32.0
27.32.1	as.bundle	12.13.32.0

Linux

Linux プラットフォームでは、本アドバイザリで説明されている脆弱性に対応するため、3 つの共有オブジェクトがアップデートされています。これらのファイルは ~/.webex directory にあります。共有オブジェクトのバージョン番号は、**ls** コマンドでディレクトリ リスティングを実行して確認できます。バージョン番号は . *so* 拡張子の後ろに記載されています。以下の表には、各共有オブジェクトの最初の修正バージョンが記載されています。インストールされているバージョンが表に記載されたバージョンまたはそれ以降であれば、システムに脆弱性はありません。

クライアント ビルド	Cisco WRF 共有オブジェクト ファイル名	共有オブジェクト ファイルのバージョン
27.32.1	libnbrascli.so	1.29.27.23
27.32.1	atjpeg.so	1.0.27.2
27.25.10	atjpeg.so	1.0.27.2

回避策

このドキュメント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

WebEx　http://support.webex.com/support/phone-numbers.html

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
http://www.cisco.com/public/sw-center/sw-usingswc.shtml

psirt@cisco.com　security-alert@cisco.com

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 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不正利用事例とその公表は確認しておりません。

この脆弱性は、Secunia および iDefense によってシスコに報告されたものです。

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

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120404-webex

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電

子メールで配信されています。

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

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-April-04	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、Cisco.com 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 Web ページには、シスコのセキュリティ アドバイザリ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。