Multiple Vulnerabilities in the Cisco WebEx Recording Format and Advanced Recording Format Players

Advisory ID: cisco-sa-20140507-webex

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140507-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 2014 May 7 16:00 UTC (GMT)

目次

要約

Cisco WebEx Recording Format（WRF）Player および Advanced Recording Format（ARF）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。これらの脆弱性が悪用されると、リモートの攻撃者が該当するプレーヤーをクラッシュさせたり、場合によってはターゲット ユーザのシステム上で任意のコードを実行することが可能になります。

これらのプレーヤーは、オンライン会議の参加者によってコンピュータに記録された WebEx 会議の内容を再生するアプリケーションです。ユーザが WebEx サーバ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。

シスコは、該当バージョンの Cisco WebEx Business Suite 会議サイト、Cisco WebEx Meetings 会議サイト、Cisco WebEx Meetings Server、Cisco WebEx WRF および ARF Player 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、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140507-webex

該当製品

脆弱性が認められる製品

このアドバイザリで公開される脆弱性は、Cisco WebEx WRF Player および Cisco WebEx ARF Player に影響を与えます。Cisco WebEx Business Suite（WBS27、WBS28、および WBS29）、Cisco WebEx Meetings (北米のみで提供)、Cisco WebEx Meetings Server 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 つ以上の脆弱性の影響を受けます。
Cisco WebEx Business Suite（WBS29）の T29.2 より前のクライアント ビルド
Cisco WebEx Business Suite（WBS28）の T28.12 より前のクライアント ビルド
Cisco WebEx Business Suite（WBS27）の T27LDSP32EP16（27.32.16）より前のクライアント ビルド
Cisco WebEx Meetings のバージョン 1.2.10 より前における、T28.12 より前のクライアント ビルド
Cisco WebEx Meetings Server の 2.0.0.1677 より前のクライアント ビルド

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。

また、Cisco WebEx Meeting クライアントから Cisco WebEx Meeting 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 プラットフォームで Cisco WebEx Meeting クライアントのバージョン情報を確認するには、 **[Help] > [About Cisco WebEx Meeting Center]** を選択します。Mac プラットフォームで Cisco WebEx Meeting クライアントのバージョン情報を確認するには、 **[Meeting Center] > [About Cisco WebEx Meeting Center]** を選択します。

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 27.32.16 が修正された場合、アップデートされたソフトウェアはビルド 27.32.17 に含まれることになります。Cisco WebEx サイト管理者は、もう 1 つのバージョン名（T27 SP32 EP16 など）でも確認することができます。この例の場合、サーバではクライアント ビルド 27.32.16 が稼働しています。

注：ソフトウェアの自動アップデートを受信していない場合、脆弱性の影響を受けるバージョンを実行している可能性がありますので、カスタマー サポートにお問い合わせください。

脆弱性が認められない製品

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。

詳細

Cisco WebEx Business Suite（WBS）会議サービスおよび Cisco WebEx Meetings は、Cisco WebEx によって管理されるホスト型マルチメディア会議ソリューションです。Cisco WebEx Meetings Server は、お客様のプライベート クラウドでホスト可能なマルチメディア会議ソリューションです。

ARF と 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。

Cisco WebEx ARF Player および Cisco WebEx WRF Player は、WebEx の ARF と WRF レコーディング ファイル（拡張子が *.arf* および *.wrf* のファイル）の再生と編集に使用されるアプリケーションです。

Cisco WebEx WRF Player および Cisco WebEx ARF Player 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、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、オフラインでレコーディング ファイルを再生することもできます。

Cisco WebEx ARF Player は、すべての Cisco WebEx 会議サイト クライアント（WBS27、WBS28、および WebEx11）と、Cisco WebEx Meetings Server クライアントで使用できます。Cisco WebEx WRF Player は、Cisco WebEx WBS 27 および WBS28 会議サイト クライアントでのみ使用でき、Cisco WebEx Meetings や Cisco WebEx Meetings Server クライアントでは使用できません。

次の表に、このアドバイザリにある脆弱性に割り当てられた Cisco Bug ID と Common Vulnerabilities and Exposures（CVE）ID を示します。

Title	CVE ID	Cisco Bug IDs
Cisco WebEx WRF and ARF Player Out of Bound Memory Read Vulnerability	CVE-2014-2132	CSCuh52768
Cisco WebEx ARF Player LZW Decompress Memory Corruption Vulnerability	CVE-2014-2133	CSCuj87565
Cisco WebEx Player WRF File Audio Channel Parsing Heap Overflow Vulnerability	CVE-2014-2134	CSCuc39458
Cisco WebEx ARF Players Memory Corruption Vulnerability	CVE-2014-2135	CSCul87216, CSCuj07603
Cisco WebEx ARF Players Memory Corruption Vulnerability	CVE-2014-2136	CSCui72223, CSCul01163, CSCul01166

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 ARF ファイルまたは 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。本セキュリティ 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。

シスコでは、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知ることができます。

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

またシスコでは、各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

CSCuh52768- Cisco WebEx WRF and ARF Players Out-of-Bounds Memory Read Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.1**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Official-Fix		Confirmed	

CSCuj87565- Cisco WebEx ARF Player LZW Decompress Memory Corruption Vulnerability 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 - **7.3**					
Exploitability		Remediation Level		Report	

		Confidence
Proof-of-Concept	Official-Fix	Confirmed

CSCuc39458- Cisco WebEx Player WRF File Audio Channel Parsing Heap Overflow Vulnerability 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 - **7.3**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Official-Fix		Confirmed	

CSCuj07603 and CSCul87216- Cisco WebEx ARF Player Memory Corruption Vulnerability 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 - **7.3**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Official-Fix		Confirmed	

CSCui72223, CSCul01163 and CSCul01166- Cisco WebEx ARF Player Memory Corruption Vulnerability 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 - **7.3**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-		Official-Fix		Confirmed	

Concept		

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、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、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

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

下記のクライアント ビルドの Cisco WebEx Business Suite（WBS27、WBS28、および WBS29）と Cisco WebEx Meetings では、このアドバイザリで説明されている脆弱性は修正されています。

- Cisco WebEx Business Suite（WBS29）の T29.2 以降のクライアント ビルド
- Cisco WebEx Business Suite（WBS28）の T28.12 以降のクライアント ビルド
- Cisco WebEx Business Suite（WBS27）の T27TLSP32EP16（27.32.16）以降のクライアント ビルド
- Cisco WebEx Meetings のバージョン 1.2.10 の T28.12 以降のクライアント ビルド
- Cisco WebEx Meetings Server の 2.0.0.1677 以降のクライアント ビルド

Cisco WebEx Business Suite の T27 SP32 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。

下記のクライアント ビルドの Cisco WebEx Meetings Server 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。

- Cisco WebEx Meetings Server の Orion 2.0 以降のクライアント ビルド

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。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 27.32.16 が修正された場合、アップデートされたソフトウェアはビルド 27.32.17 に含まれることになります。

このアドバイザリで公開される脆弱性は、Cisco WebEx WRF Player および ARF Player に影響を与えます。各プレーヤーの Microsoft Windows、Apple Mac OS X、Linux のすべてのバージョンが、このアドバイザリに記載されている脆弱性のうち少なくとも 1 つの影響を受けます。Cisco WebEx ARF Player または Cisco WebEx WRF Player 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。Cisco WebEx ARF Player または Cisco WebEx

WRF Player 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。

インストールされたプレーヤーが脆弱性による影響を受けるバージョンであるかを確認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。

Microsoft Windows

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、Microsoft Windows プラットフォームでは 10 個のダイナミック リンク ライブラリ (DLL) が更新されています。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、各 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。

Client Build	Cisco DLL Filename	DLL File Versions
T28	atas32.dll	28, 0800, 0012, 1105
T28	Atjpeg60.dll	2028,1208,1100,500
T28	atas32_lite.dll	28, 0800, 0112, 1105
T28	atdl2006.dll	1028, 1208, 1100, 0500
T28	atpdmod.dll	2028.1208.1100.2300
T28	nbrpd.dll	2028.1208.1100.2300
T28	atprtses.dll	2028.1208.1100.2300
T28	atprtsc.dll	2028.1208.1100.2300
T27LDSP32EP16	atjpg60.dll	1027,1232,1016,2200
T27LDSP32EP16	atas32.dll	1027,1232,1016,2200
T27LDSP32EP16	Atas32_Lite.dll	1027,1232,1016,2201
T27LDSP32EP16	atdl2006.dll	1027,1232,1016,2300
T27LDSP32EP16	atpdmod.dll	2029.1232.1116.2300
T27LDSP32EP16	nbrpd.dll	2029.1232.1116.2300
T27LDSP32EP16	atprtses.dll	2029.1232.1116.2300
T27LDSP32EP16	atprtsc.dll	2029.1232.1116.2300
T29L10N	nbrpse.dll	2029.1311.900.1100
Orion2.0.0.FCS	nbrpse.dll	2029.1332.1200.600

Apple Mac OS X

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、6 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、Ctrl を押しながらファイル名をクリックします。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。

Client Build	Cisco Bundle Filename	Bundle File Versions
T28	as.bundle	1211.5.2808.0
T28	atas.bundle	1211.5.2808.0
T28	asplayback.bundle	1211.5.2808.0
T28	pd.bundle	1211.20.2808.0
T28	nbrpd.bundle	1211.20.2808.0
T27LDSP32EP16	as.bundle	1210.24.2732.16
T27LDSP32EP16	atas.bundle	1210.24.2732.16
T27LDSP32EP16	asplayback.bundle	1210.24.2732.16
T27LDSP32EP16	pd.bundle	1211.15.2732.16
T27LDSP32EP16	nbrpd.bundle	1211.15.2732.16
T29L10N	nbrpse.bundle	1309.11.2900.0
Orion2.0.0.FCS	nbrpse.bundle	1312.06.2732.201

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、8 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* の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。Cisco WebEx Meetings Server は Linux クライアントではサポートされないため、この製品は表に記載されていません。

Client Build	Cisco Shared Object Filename	Shared Object File Versions
T28	WRF player AS	1.0.28.19
T28	NBR Player AS	1.0.28.18
T28	Meeting AS	922800026
T28	libatdv.so	922800010
T28	libnbrdv.so	1.0.28.19
T27LDSP32EP16	WRF player AS	1.29.27.28
T27LDSP32EP16	NBR Player AS	1.29.27.23
T27LDSP32EP16	libatdv.so	922700067
T27LDSP32EP16	libnbrdv.so	1.0.27.23
T29L10N	nbrpse.so	1.0.29.3

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が、http://support.webex.com/support/downloads.html にある Meeting Services Removal Tool（Microsoft Windows ユーザの場合）または Mac Cisco-WebEx Uninstaller（Apple Mac OS X

ユーザの場合）を利用して、すべての WebEx ソフトウェアをシステムから完全に削除することができます。

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://support.webex.com/MyAccountWeb/knowledgeBase.do?root=Tools&parent=Knowledge&articleId=WBX28548&txtSearchQuery=uninstall%20linux# にある WebEx ナレッジ ベースのヘルプ記事に記載された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の入手

このセクションは、Cisco WebEx Meetings Server 製品の脆弱性と、Cisco WebEx Business Suite サービスに適用されます。

シスコでは、これらの脆弱性に対応するため、Cisco WebEx WRF Player および Cisco WebEx ARF Player の該当バージョンをアップデートしました。Cisco WebEx Business Suite（WBS27、WBS28、および WBS29）サービスをご使用のお客様の大半は、このアップデートを自動的に受信することができます。最新のセキュリティ アップデートをまだ受信していないお客様は、Customer Success 担当者に連絡して、アップグレードの計画を始めることが可能です。Cisco WebEx Meetings サービスをご使用のすべてのお客様は、このアップデートを自動的に受信できます。

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 Cisco WebEx Meetings Server ソフトウェア アップデートを無償で提供しています。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の特有の問題をご確認ください。

質問や追加のサポートが必要な場合、またはフィードバックの提供、最新リリースについての質問がある場合は、Cisco WebEx グローバル サポート サービスおよびテクニカル サポートまでお問い合わせください。その際は、 http://support.webex.com/support/support-overview.html にアクセスするか、+1-866-229-3239 または +1-408-435-7088 にご連絡ください。米国以外に在住の場合は、 http://support.webex.com/support/phone-numbers.html にアクセスして各地域のサポート番号をご確認ください。

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。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

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 Meetings Server 製品の脆弱性にのみ適用されます。

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレ

ードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

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 Meetings Server 製品の脆弱性にのみ適用されます。

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

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 Meetings Server 製品の脆弱性にのみ適用されます。

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、E メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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、Fortinet、iDefense、および Microsoft Vulnerability Research（MSVR）によって下記のとおりに報告されたものです。

Cisco Bug IDs	Reporter
CSCuh52768, CSCuj87565, CSCui72223, CSCul01163, CSCul01166	Fortinet

CSCuc39458	iDefense
CSCul87216, CSCuj07603	MSVR

シスコは、この脆弱性を報告いただき、弊社と連携しての公開にご協力いただいたことに対して、各機関に感謝いたします。

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-20140507-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 E 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

本アドバイザリに関する今後の更新は 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。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-May-07	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してくださ

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。