Cisco Security Advisory: Cisco Unified Contact Center Express Directory Traversal Vulnerability

Advisory ID: cisco-sa-20111026-uccx

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

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 Unified Contact Center Express (UCCX または Unified CCX) および Cisco Unified IP Interactive Voice Response (Unified IP-IVR) には、ディレクトリ トラバーサルの脆弱性が存在します。これにより、認証されていない攻撃者がリモートからファイルシステム内の任意のファイルを取得できる可能性があります。

シスコはこの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ました。

この脆弱性を軽減する対応策はありません。

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-uccx

Cisco Unified Communications Manager もこの脆弱性の影響を受けます。これについては別途アドバイザリが公開されています。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-cucm

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

脆弱性が存在する製品

次の Cisco UCCX バージョンに脆弱性が含まれています。

- Cisco UCCX バージョン 6.0(x)
- Cisco UCCX バージョン 7.0(x)
- Cisco UCCX バージョン 8.0(x)
- Cisco UCCX バージョン 8.5(x)

注：バージョン 6.0(x) より前の Cisco UCCX はソフトウェア メンテナンスが終了しています。6.0(x) より前のバージョンを使用している場合は、Cisco UCCX のサポートされているバージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

次の Cisco Unified IP Interactive Voice Response バージョンには脆弱性が含まれています。

- Cisco Unified IP Interactive Voice Response バージョン 6.0(x)
- Cisco Unified IP Interactive Voice Response バージョン 7.0(x)
- Cisco Unified IP Interactive Voice Response バージョン 8.0(x)
- Cisco Unified IP Interactive Voice Response バージョン 8.5(x)

注：6.0(x) より前のバージョンの Cisco Unified IP Interactive Voice Response は、ソフトウェア メンテナンスが終了しています。6.0(x) より前のバージョンを使用している場合は、Cisco Unified IP Interactive Voice Response のサポートされているバージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

脆弱性が存在しない製品

Cisco Unified Communications Manager を除いて、この脆弱性の影響を受けるシスコ製品は現在確認されていません。

詳細

Cisco Unified Contact Center Express は単一および 2 ノードのサーバで、多数の エージェントをサポートするために統合された「コンタクト センター イン ア ボックス（Contact Center-in-a-Box）」ソリューションです。8.0(x) およびそれより前のバージョンでは最大 300 エージェント、バージョン 8.5(x) 以降は 400 エージェントに対応します。

Cisco Unified Interactive Voice Response は UCCX 製品パッケージで、コンタクトセンター向けの IP コール キューイングおよび IP インテリジェント音声応答機能を提供します。

Cisco Unified Communications Manager および Cisco Unified Contact Center Express のディレクトリ トラバーサルの脆弱性
Cisco Unified Communications Manager、Cisco Unified Contact Center Express、および Cisco Unified IP Interactive Voice Response には、ディレクトリ トラバーサルの脆弱性が存在します。これにより、認証されていない攻撃者がリモートからファイルシステム内の任意のファイルを取得できる可能性があります。

この脆弱性は、入力に対する不適切な検証に起因し、攻撃者はファイルシステムのディレクトリを通過できる可能性があります。攻撃者は巧妙に細工された URL を該当システムに送信することで、この脆弱性を不正利用できる可能性があります。

Cisco Unified Contact Center Express および Cisco Unified IP Interactive Voice Response の脆弱性は、該当製品のバージョン 6.0(x) および 7.0(x) の TCP ポート 8080 と、8.0(x) 以降のバージョンの TCP ポート 9080 で不正利用される可能性があります。

注：Cisco Unified Contact Center Express および Cisco Unified IP Interactive Voice Response のバージョン 6.0(x) および 7.0(x) では、サーバ側でポート 8080 の再設定を行うことができます。

このアドバイザリに説明されている Cisco Unified Contact Center Express および Cisco Unified IP Interactive Voice Response の脆弱性は、Cisco Bug ID CSCts44049 （ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-3315 が割り当てられています。

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

CSCts44049, UCCX vulnerable to directory traversal Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Low	None	Complete	None	None
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、認証されていない攻撃者がリモートから Cisco Unified Contact Center Express または Cisco Unified IP Interactive Voice Response のファイルシステム内にある任意のファイルを取得できる可能性があります。

ソフトウェア バージョンおよび修正

シスコはこの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ました。

次の表に、Cisco Unified Contact Center Express および Cisco Unified IP Interactive Voice Response の該当バージョンそれぞれに対する修正を記載します。

Version	First Fixed in
6.0(x)	6.0(1)SR1ES8
7.0(x)	7.0(2)ES1
8.0(x)	8.0(2)SU3 and patch ciscouccx.802SU3_CSCts44049.cop.sgn
8.5(x)	8.5(1)SU2

リリース 6.0(1)SR1ES8 および 7.0(2)ES1 は cisco.com に掲載されません。Cisco Technical Assistance Center（TAC）までお問い合わせください。

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。

回避策

この脆弱性に対する回避策はありません。ネットワーク内のシスコ デバイスに適用可能な対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。 http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20111026-cucm-uccx

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

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。大半のお客様は、 http://www.cisco.com にあるシスコの Web サイトの Software Center からアップグレードを入手できます。

サードパーティのサポート会社をご利用のお客様

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、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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、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を入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお知らせの 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に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 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 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、Digital Defense, Inc.社 の Vulnerability Research Team から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

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-uccx

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。