# Cisco Unified Communications Web ベースの管理の脆弱性


アドバイザリーID : cisco-sa-20071017-IPCC
初公開日 : 2007-10-17 16:00
バージョン 1.1 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2007-5539

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

Unified Contact Center および Intelligent Contact Management の各製品には、Web ベースのレポート作成とスクリプト監視ツール（Web View）や Web ベースの設定ツール（Web Admin）への不正アクセスの原因となる可能性がある脆弱性が含まれています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071017-IPCC で公開されています。

## 該当製品

### 脆弱性のある製品

次の製品は、Web ベースのレポート作成とスクリプト監視ツール（Web View）への不正アクセスの原因となる脆弱性に該当します。

- Cisco Unified Intelligent Contact Management Enterprise（Unified ICME）
- Cisco Unified ICM Hosted（Unified ICMH）
- Cisco Unified Contact Center Enterprise（UCCE）
- Cisco Unified Contact Center Hosted（UCCH）
- Cisco System Unified Contact Center Enterprise（SUCCE）

次の製品は、Web ベースの設定ツール（Web Admin）への不正アクセスの原因となる脆弱性に該当します。

- Cisco System Unified Contact Center Enterprise（SUCCE）

Administration Workstation（AW）にインストールされたソフトウェアのバージョンを調べるには、Windows Server の Add or Remove Programs ウィンドウに移動します。影響を受けている場合、インストールされているアプリケーションの一覧に Cisco ICM Maintenance Release ICM 7.1(5) と表示されます。

### 脆弱性を含んでいないことが確認された製品

次の製品は、このドキュメントで説明されている脆弱性には該当しません。

- Cisco Unified Contact Center Express
- Cisco IP Contact Center Express

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかっていません。

この脆弱性が該当するのは、ソフトウェア バージョン ICM 7.1(5) が稼働している確認済みの製品だけです。

## 詳細

Cisco Unified ICME、Unified ICMH、UCCE、UCCH、および SUCCE は、戦略的プラットフォームのスイートであり、これらを使用すると、複数の通信チャネルのブレンディングを使用した、インテリジェントなルーティングとコール処理が可能になります。

Cisco Unified ICME、Unified ICMH、UCCE、UCCH、および SUCCE の各エディションのソフトウェア バージョン 7.1(5) には、Windows Active Directory ドメインが定義されたユーザによる不正な特権レベルの取得を可能にする脆弱性が存在します。このため、Windows Active Directory ユーザは、任意のコール センター インスタンスの Web View レポート情報を表示することができるようになります。Cisco SUCCE も Web Admin ツールへの不正アクセスによる影響を受け、アプリケーション権限の編集などのアプリケーション設定の変更が可能になる可能性があります。

この脆弱性は、Cisco Bug ID CSCsj55686(登録ユーザ専用)に記載されています。

## 回避策

ICM/IPCC Active Directory 階層に属していない Active Directory で定義された Windows ユーザに、Web View および Web Admin の各ツールへの完全なアクセス権が与えられます。回避策はありません。IPCC サーバが常駐する Windows Active Directory ドメインで定義され、ICM/IPCC Active Directory 階層のインスタンスに関連付けられたユーザは、適切な許可が与えられます。信頼できるホストからだけの Administration Workstation へのアクセスを許可するために、Transit ACL などのフィルタを使用できます。

TCP ポート 80 を使用している HTTP パケットおよび TCP ポート 443 を使用している HTTPS パケットを拒否するフィルタは、入力アクセス ポイントからネットワーク内に進入するトラフィ

ックを保護するために、tACL ポリシーの一部としてネットワーク全体に展開される必要があります。フィルタが適用されるデバイスとその背後にある他のデバイスを保護するには、このポリシーを設定する必要があります。TCP ポート 80 を使用している HTTP パケットと TCP ポート 443 を使用している HTTPS パケットのフィルタは、信頼できるクライアントからのトラフィックだけが許可されるように、脆弱性のあるネットワーク デバイスの直前に展開される必要もあります。

tACLについての詳細は、『トランジットアクセスコントロールリスト：エッジでのフィルタリング
：http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml』を参照してください。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20071017-IPCC)を参照してください。

## 修正済みソフトウェア

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機器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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

| ソフトウェア リリース | パッチ | メンテナンス |
|---|---|---|
| 7.1(5) | ICM7.1(5)_ES46 | 7.2(3)（2007 年 12 月 リリース） |

Contact Center および ICM メンテナンス ソフトウェアは、次の URL からダウンロード可能です。

https://sec.cloudapps.cisco.com/support/downloads/go/MDFTree.x?butype=cc（登録ユーザ専用）

## 推奨事項

$propertyAndFields.get("recommendations")

## 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やその公表は確認しておりません。

この脆弱性は、カスタマー サポートのサービス リクエストの解決中に発見されたものです。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071017-IPCC

## 改訂履歴

| | | |
|---|---|---|
| リビジョン 1.1 | 2008年4月25日 | CSCsj55686のCVSSスコアへのリンクを更新。 |
| リビジョン 1.0 | 2007 年 10 月 17 日 | 初版リリース |

## 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。