Multiple Vulnerabilities in Cisco Unified Communications Manager

Advisory ID: cisco-sa-20130717-cucm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-cucm

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 1.1

Last Updated 2013 July 17 18:00 UTC (GMT)

For Public Release 2013 July 17 16:00 UTC (GMT)

目次

要約

Cisco Unified Communications Manager（Unified CM）には、複数の脆弱性があり、それらを組み合わせて使用することにより、不正な攻撃者がリモートでユーザ資格情報を収集し、権限をエスカレーションしたり、コマンドを実行して脆弱なシステムを完全に制御したりすることができます。攻撃に成功すると、不正な攻撃者が Cisco Unified CM の情報にアクセスし、情報を作成したり、変更したりすることができます。

2013 年 6 月 6 日に、フランスのセキュリティ企業である Lexfo 社が、Cisco Unified CM の改ざんに使用される複数の脆弱性のデモを含む VoIP セキュリティの公開プレゼンテーションを行いました。プレゼンテーションの間、研究者が一連の脆弱性をいくつかの段階に分けて攻撃し、Cisco Unified CM サーバの完全な改ざんに成功しました。一連の攻撃では、次のタイプの脆弱性を使用しました。

- ブラインド SQL（Structured Query Language）インジェクション

- コマンド インジェクション
- 権限のエスカレーション

シスコ PSIRT では、研究者と協力してセキュリティ脆弱性に関する調査を進め、製品レポートで発表することを常に歓迎しています。

シスコはこのアドバイザリに記載された脆弱性のうち 3 つに対処する Cisco Options Package (COP) ファイルを提供しています。シスコは現在、残りの脆弱性について調査中です。これらの脆弱性を軽減する回避策はありません。

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-20130717-cucm

該当製品

脆弱性が認められる製品

次の製品は、このアドバイザリに記載される脆弱性の影響を受けます。

- Cisco Unified Communications Manager 7.1(x)
- Cisco Unified Communications Manager 8.5(x)
- Cisco Unified Communications Manager 8.6(x)
- Cisco Unified Communications Manager 9.0(x)
- Cisco Unified Communications Manager 9.1(x)

注：Cisco Unified CM バージョン 8.0 は 2012 年 10 月 23 日にソフトウェア メンテナンスが終了しています。Cisco Unified CM 8.0(x) バージョンをご利用のお客様は、サポートされている Cisco Unified CM の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。

本文書に記載されている脆弱性が確認されている製品は Cisco Unified CM のみです。その他の音声製品も、本文書に記載されている脆弱性の一部の影響を受ける可能性があります。次の製品は調査中ですが、脆弱性としては確認されていません。

- Cisco Emergency Responder
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified Presence Server/Cisco IM and Presence Service
- Cisco Unity Connection

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脆弱性の影響を受けるものは、現在確認されていません。

詳細

Cisco Unified CM は、IP Phone、メディア処理デバイス、VoIP ゲートウェイ、およびマルチメディア アプリケーションなどのパケット テレフォニー ネットワーク デバイスにエンタープライズ テレフォニー機能を拡張する、シスコ IP テレフォニー ソリューションのコール処理コンポーネントです。

ブラインド SQL (Structured Query Language) インジェクションに関する脆弱性

Cisco Unified CM および関連製品には、次のブラインド SQL インジェクションの脆弱性のうち、

1 つ以上が含まれる場合があります。この脆弱性は、特定の脆弱性に応じて、認証済みまたは認証されていないコンテキストから不正利用される可能性があります。

SQL インジェクションの脆弱性は、SQL クエリーの作成で使用される前に、ユーザが提供したリクエストを適切に検証できないことにより発生するものです。攻撃者は、SQL コマンドをインジェクトすることにより、この動作を不正利用できます。不正利用により、攻撃者はデータベース内の任意の情報の漏えいや変更が可能です。

特定された最初の脆弱性は、不正な攻撃者によりリモートで不正利用される場合があります。不正利用により、攻撃者はメタデータを使用して、データベース内の暗号化情報を再作成できます。このメタデータは、暗号化情報の再構築に使用される場合があります。

この脆弱性は、Cisco Bug ID CSCuh01051（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-3404 が割り当てられています。この脆弱性は、Cisco Unified CM バージョン 9.1(1a) 以前に該当します。

2 番目の脆弱性は、認証済みの攻撃者にリモートで不正利用される場合があります。不正利用により、攻撃者はデータベース内の特定のテーブルに対して追加情報を変更したり、挿入したりすることができます。

この脆弱性は、Cisco Bug ID CSCuh81766（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3412 が割り当てられています。この脆弱性は、Cisco Unified Communications Manager versions 9.1(2) 以前に該当します。

これらの脆弱性は、デフォルトの管理ポートである TCP ポート 8080 または 8443 で不正利用される可能性があります。

ハードコードされた暗号キー

Cisco Unified Communications Manager（Unified CM）には、データベースに保存されている機密データの暗号化に使用されるハードコードされた暗号キーとともに、Computer Telephony Integration（CTI）通信のセキュリティが含まれます。

この問題は、Cisco Unified CM の全バージョンの静的対称暗号キーの使用により発生するものです。攻撃者は、秘密キーを使用して、ユーザ資格情報を含む機密データを復号化することによって、この問題を不正利用します。この不正利用により、攻撃者は他の攻撃によって入手したユーザ資格情報などの機密システム情報を復号化できます。 この問題は、Cisco Bug ID の CSCsc69187（ 登録ユーザ専用 ）に記述されています。この問題は、Cisco Unified Communications Manager バージョン 9.1(2) 以前に該当します。

Cisco Unified Presence Server/IM & Presence Service バージョン 9.1(2) 以前もこの問題の影響をうけます。この問題は、Cisco Bug ID の CSCui01756（ 登録ユーザ専用 ）に記述されています。

コマンド インジェクションに関する脆弱性

Cisco Unified Communications Manager（Unified CM）の脆弱性により、不正な攻撃者がリモートで、データベース ユーザの権限を使用して、基盤 OS でコマンドを実行することができます。

この脆弱性は、ユーザによる入力を適切に検証できないことにより発生するものです。攻撃者は、該当する機能に不正な入力を送信することで、この脆弱性を不正利用できます。

この脆弱性は、Cisco Bug ID CSCuh73440（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3402 が割り当てられています。この脆弱性は、Cisco Unified Communications

Manager versions 9.1(2) 以前に該当します。

権限エスカレーションに関する脆弱性

Cisco Unified Communications Manager の脆弱性により、認証済みの攻撃者がローカルで、システムの権限をエスカレーションできます。

この脆弱性は、権限のあるシステム スクリプトまたはバイナリにおける不適切なファイルの許可、環境変数、および関連パスによるものです。攻撃者は、システム スクリプトを変更することによって、この脆弱性を不正利用できます。これにより、攻撃者は該当するシステムを完全に制御できます。

権限エスカレーションに関する脆弱性の最初の 2 つは Cisco Bug ID CSCuh73454（ 登録ユーザ専用 ）および CSCuh87042（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3403 が割り当てられています。

3 番目の脆弱性は、Cisco Bug ID CSCui02242（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3434 が割り当てられています。

4 番目の脆弱性は、Cisco Bug ID CSCui02276（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3433 が割り当てられています。

この脆弱性は、Cisco Unified CM バージョン 9.1(1a) 以前に該当します。

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。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/

CSCuh01051- Cisco Unified Communications Manager Blind SQL Injection Vulnerability Calculate the environmental score of					
CVSS Base Score - **6.4**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Low	None	Partial	Partial	None
CVSS Temporal Score - **5.5**					
Exploitability		Remediation Level		Report Confidence	
Functional		Temporary-Fix		Confirmed	

CSCuh81766- Cisco Unified Communications Manager Blind Structured Query Language Injection Vulnerabilities Calculate the environmental score of					
CVSS Base Score - **5.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Partial	Partial	None
CVSS Temporal Score - **5.2**					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

CSCuh73454 and CSCuh87042- Cisco Unified Communications Manager Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **6.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **5.5**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Temporary-Fix		Confirmed	

CSCuh73440 - Cisco Unified Communications Manager Command Injection Vulnerability Calculate the environmental score of					
CVSS Base Score - **6.5**					
Acces	Access	Authentica	Confidenti	Integr	Availabi

s Vecto r	Comple xity	tion	ality Impact	ity Impa ct	lity Impact
Netw ork	Low	Single	Partial	Partia l	Partial
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Unavailable		Confirmed	

CSCui02242 - Cisco Unified Communications Manager Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **6.8**					
Acce ss Vect or	Access Comple xity	Authentica tion	Confidenti ality Impact	Integrit y Impact	Availabi lity Impact
Local	Low	Single	Complete	Compl ete	Comple te
CVSS Temporal Score - **6.1**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Unavailable		Confirmed	

CSCui02276 - Cisco Unified Communications Manager Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **6.8**					
Acce ss Vect or	Access Comple xity	Authentica tion	Confidenti ality Impact	Integrit y Impact	Availabi lity Impact
Local	Low	Single	Complete	Compl ete	Comple te
CVSS Temporal Score - **6.1**					
Exploitability		Remediation Level		Report Confidence	
Proof-of-Concept		Unavailable		Confirmed	

注：ハードコードされた静的暗号キーは、脆弱性ではなく困難な問題と見なされるため、CVSS スコアは 0/0 となります。

影響

ブラインド SQL インジェクションの脆弱性の不正利用に成功すると、攻撃者がリモートで暗号化情報を再構築し、Cisco Unified CM データベース内に行を挿入できます。最初のブラインド SQL インジェクションにより、不正な攻撃者がハードコードされた暗号キーをリモートで使用し、ローカル ユーザ アカウントを入手および復号化できます。これにより、後続の認証済みブラインド SQL インジェクションが可能になります。

コマンド インジェクションの不正利用の成功と権限エスカレーションの脆弱性により、認証済みの攻撃者が特権権限を使用して、基盤 OS で任意のコマンドをリモートで実行できます。

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。

現時点では、このアドバイザリに記載された脆弱性に対するソフトウェア修正を含む Cisco Unified CM バージョンは存在しません。修正済みソフトウェアが入手可能になり次第、このアドバイザリは更新されます。それまでの間の対策として、シスコは次の脆弱性（ **CSCuh01051**、**CSCuh87042**、 **CSCuh73454** ）に対処する Cisco Options Package（COP）ファイルを提供しています。

お客様は以前の脆弱性への対処としてこの COP ファイルをダウンロードしてインストールし、問題が修正されたバージョンのソフトウェアが提供されるのを待つことができます。

このパッケージは、次のシステム バージョンにインストールされます。

- 7.1.3
- 7.1.5
- 8.5.1
- 8.6.2
- 9.1.1

COP ファイル（ *cmterm-CSCuh01051-2.cop.sgn* ）は、上記の各バージョンの ソフトウェア ダウンロード ページの「ユーティリティ」セクションにあります。たとえば、9.1(x) バージョンのファイルは、ソフトウェア ダウンロード ページの次のパスに移動することによって見つけ出すことができます。

Products -> Voice and Unified Communications -> IP Telephony -> Unified Communications Platform -> Cisco Unified Communications Manager -> Cisco Unified Communications Manager Version 9.1 -> Unified Communications Manager / CallManager / Cisco Unity Connection Utilities-COP-Files

この COP は初期攻撃（CSCuh01051）を回避し、本文書に記載されている脆弱性の攻撃個所を制限できます。影響を受けるすべての Cisco Unified CM バージョンに COP ファイルを適用する

ことを強く推奨します。

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。

追加の回避策の詳細については、次の場所にある付属の『Applied Mitigation Bulletin（AMB）』で参照できます： http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=29846

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された 3 つの脆弱性に対処する COP ファイルを提供しています。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の特有の問題をご確認ください。

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。

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。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。 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

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

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。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

このブラインド SQL インジェクションに関する脆弱性（CSCuh01051）は、Emerging Defense 社によりシスコに最初に報告されました。

これらの脆弱性は、6 月 6 日にフランスのレンヌで開催された SSTIC 2013 IT セキュリティ会議において、フランスのセキュリティ企業である Lexfo 社によってデモンストレーションされました。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いかなる不正利用事例も確認しておりません。

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-20130717-cucm

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 1.1	2013-July-17	Corrected CVSS score to correct the remediation level for privilege escalation vulnerabilities CSCuh73454 and CSCuh87042 (CVE-2013-3403).Two minor wording corrections for clarity.

Revision 1.0	2013-July-17	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/en/US/products/products_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。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。