Cisco Unified Communications Managerのリモートブラインド SQLインジェクションの脆弱性

アドバイザリーID : Cisco-SA-20130717-CVE-2013-3404
CVE-2013-3404
初公開日 : 2013-07-17 16:07
バージョン 1.0 : Final
CVSSスコア : 6.4
回避策 : No Workarounds available
Cisco バグ ID : CSCuh01051

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

Cisco Unified Communication Manager(Unified CM)には、認証されていないリモートの攻撃者がブラインドStructured Query Language(SQL)インジェクションを実行する可能性のある脆弱性が存在します。

この脆弱性は、Cisco Unified CMによるユーザ指定の要求の検証が不適切なことに起因します。攻撃者は、SQLコマンドを挿入することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はメタデータを活用してデータベース内に暗号化された情報を再作成できる可能性があります。このメタデータは、暗号化されたクレデンシャルの再構築に使用できます。

この脆弱性の不正利用のデモを実施するための概念実証コードが公開されています。

シスコはセキュリティアドバイザリでこの脆弱性を確認し、一時的な修正をリリースしました。

この脆弱性を不正利用するには、攻撃者が信頼できる内部ネットワークにアクセスし、巧妙に細工された要求を該当ソフトウェアに送信する必要がある場合があります。このアクセス要件により、エクスプロイトが成功する可能性が制限される可能性があります。

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)バージョンをご使用のお客様は、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。

脆弱性が確認されている製品はCisco Unified CMのみです。その他の音声製品は、アドバイザリに記載されている個別の脆弱性の1つ以上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、脆弱性が存在すること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サービス
- Cisco Unity Connection

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

該当製品

シスコは、Bug ID CSCuh01051のセキュリティアドバイザリを次のリンクでリリースしました。cisco-sa-20130717-cucm

脆弱性のある製品

Cisco Unified CMバージョン9.1(1a)以前が影響を受けます。

脆弱性を含んでいないことが確認された製品

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。

回避策

適切なアップデートを適用することを推奨します。

今後のアップデートやリリースについては、ベンダーに問い合わせることをお勧めします。

Cisco Applied Intelligenceチームは、更新されたソフトウェアを適用する前に、この脆弱性を悪用しようとする攻撃を識別して緩和するために管理者をガイドする次の関連文書を作成しました：Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Unified Communications Manager

SQLインジェクションの攻撃と防御の詳細については、「SQLインジェクションについて」を参照してください。

管理者は、信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

管理者は、IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけが該当システムにアクセスできるようにすることを検討できます。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

契約が有効なシスコのお客様は、 Software Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、 tac@cisco.comの電子メールでアップグレードを入手できます。

該当ソフトウェアのユーティリティセクションのソフトウェアダウンロードページに、Cisco Options Package(COP)ファイル cmterm-CSCuh01051-2.cop.sgnがリリースされています。9.1(x)バージョン用のCOPファイルは、ソフトウェアダウンロードページで次のパスに移動すると見つかります。

[製品] > [音声およびユニファイドコミュニケーション] > [IPテレフォニー] > [ユニファイドコミュニケーションプラットフォーム] > [Cisco Unified Communications Manager] > [Cisco Unified Communications Managerバージョン9.1] > [Unified Communications Manager/CallManager/Cisco Unity Connection Utilities-COP-Files]

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20130717-CVE-2013-3404

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2013年7月17日

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり

する権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。