Cisco Unity Connection Webインターフェイス SQL インジェクション脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150918-CVE-2015-6299 **初公開日 :** 2015-09-18 20:25 **最終更新日 :** 2015-09-21 17:26 **バージョン 2.0 :** Final **CVSSスコア :** 6.5 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2015-6299

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 Unity Connection （ UC ）の Webインターフェイスの脆弱性は任意 SQL クエリの実行によってシステムの機密保持に影響を与える認証される、リモート攻撃者可能にする可能性があります。

脆弱性は SQL クエリのユーザが指定する入力の入力の検証の欠如が原因です。 攻撃者は HTTP POST 要求パラメータとして SQL コマンドが含まれている悪意をもって 巧妙に細工された値の入力によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者がデータベースのある特定の値の存在を判別することを可能にする可能性があります。

Cisco は脆弱性を確認しました; ただし、ソフトウェア アップデートは利用できません。

この脆弱性を不正利用するために、攻撃者は目標とされたデバイスに認証する必要があります。このアクセス要件は正常なエクスプロイトの確率を下げるかもしれません。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

この脆弱性は NCIA/NCIRC からのポール Heneghan によって Cisco に報告されました。

該当製品

Cisco は影響を受けた製品バージョンの追加詳細および最新リストが含まれている登録ユーザ向けのバグID CSCuv63824 をリリースしました。

脆弱性のある製品

このアラートが最初に送達された時、Cisco Unity Connection バージョン 9.1(1.2) は前に脆弱であり。 以降のバージョンはまた脆弱かもしれません。

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

管理者は今後のアップデートおよびリリースに関するベンダーに連絡するように助言されます。

管理者は信頼されたユーザだけネットワーク アクセスをアクセスできることを許可するために助言されます。

管理者は特権ユーザだけ管理か管理 システムにアクセスすることを許可するために助言されます。

SQL インジェクション不正侵入および防御についてのその他の情報に関しては、知識 SQL インジェクションを参照して下さい。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

ソフトウェア アップデートは利用できません

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エクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150918-CVE-2015-6299

改訂履歴

Version	Description	Section	Status	日付

1.0	Cisco Unity Connection は認証される可能にする可能性がある SQL インジェクション不正侵入を行なうために脆弱性がリモート攻撃者含まれています。 更新は利用できません。	該当なし	Final	2015-Sep-18

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。