

Cisco Unified Communications Manager SQL インジェクション脆弱性

Medium	アドバイザリーID : cisco-sa-20170802-ucm	CVE-2017-6757
m	初公開日 : 2017-08-02 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.4	
	回避策 : Yes	
	Cisco バグ ID : CSCve13786	

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 Communications Manager の脆弱性は盲目 SQL インジェクション 攻撃を行なう認証される、リモート攻撃者可能にする可能性があります。

脆弱性は保護フィルターをバイパスする SQL クエリで使用されるユーザが指定する入力を検証する失敗が原因です。攻撃者は SQL 文を含む巧妙に細工された URL の送信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の統合に影響を与えるいくつかのデータベーステーブルの Delete エントリが修正するようにする可能性があります。

この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-ucm>

影響を受ける製品

脆弱性が存在する製品

この脆弱性は Cisco Unified Communications Manager に影響を与えます。該当するソフトウェアリリースについての情報に関しては、このアドバイザリーの上で Cisco バグ ID を参照して下さい。

脆弱性が存在しない製品

他のシスコ製品において、このアドバイザリーの影響を受けるものは現在確認されていません。

細部

回避策

この脆弱性に対処する回避策はありません。

固定ソフトウェア

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

ソフトウェアのアップグレードを検討する際には、[Cisco Security Advisories and Alerts ページ](#)で入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性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。

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。

ソース

この脆弱性は名前を挙げられたいと思わない外部研究者によって発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-ucm>

改訂履歴

Version	Description	Section	Status	Date
1.0	Initial public release.		Final	2017-August-02

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、単独の転載や意識を施した場合、

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。