ユーザ認証が失敗する場合の CTI の LDAP 接続リーク

severity	**アドバイザリーID :** cisco-sa-20020327-cm-ctifw-leak **初公開日 :** 2002-03-27 17:00 **バージョン 1.1 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2002-0505

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

CTI フレームワーク 認証のメモリリークによりサーバはリロードという結果にクラッシュし、終ります場合があるかある特定のソフトウェア リリースを実行する Cisco Unified CallManager に脆弱性があります。 この脆弱性がサービス拒絶（DoS）攻撃を始めるのに不正利用することができます。

この脆弱性は Cisco バグ ID CSCdv28302 として文書化されています。 利用可能 な 回避策が脆弱性を軽減するためにあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020327-cm-ctifw-leak で利用できます。

該当製品

修正済みソフトウェア

製品に脆弱性があるかどうかについては、以下のリストを確認してください。 ソフトウェアバージョンまたは設定情報が示されている場合は、その組み合せにのみ脆弱性があります。

- Cisco CallManager 3.1

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。

改訂履歴

リビジョン 1.1	2002-Mar-28	訂正された最初修正済みリリース
リビジョン 1.0	2002-Mar-27	初版リリース

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。