



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
*Agence nationale de la sécurité
des systèmes d'information*
CERTA

Paris, le 28 mars 2002
N° CERTA-2002-AVI-064

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de sur CISCO Call Manager 3.1

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-064>

Gestion du document

Référence	CERTA-2002-AVI-064
Titre	Vulnérabilité de CISCO CallManager 3.1
Date de la première version	28 mars 2002
Date de la dernière version	-
Source(s)	Bulletin de sécurité de CISCO
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

CISCO CallManager 3.1.

3 Résumé

Un utilisateur mal intentionné peut redémarrer à distance un appareil CISCO au moyen d'une fuite de mémoire du logiciel CallManager.

4 Description

CISCO CallManager est un composant logiciel permettant d'effectuer des appels téléphoniques en voix sur IP.

Le logiciel CISCO Call Manager 3.1 possède une fuite de mémoire dans le processus d'authentification d'un utilisateur du CTIFW (*Call Telephony Integration FrameWork*). Cette faille permet à un utilisateur distant mal intentionné de consommer les ressources du système jusqu'à provoquer un redémarrage de l'appareil.

5 Contournement provisoire

- Si le logiciel CallManager a été installé mais n'est pas utilisé sur vos appareils CISCO, le supprimer.
- S'il est en cours d'utilisation suivre les instructions données sur le site de CISCO :
http://www.cisco.com/univercd/cc/td/doc/product/voice/c/callmg/3_0/install/ad_3011.htm#xtocid30717

6 Solution

Passer à la version 1.3(2) de CISCO CallManager présente sur le site :
<http://www.cisco.com>

7 Documentation

Bulletin de sécurité CISCO :
<http://www.cisco.com/warp/public/707/callmanager-ctifw-leak-pub.shtml>

Gestion détaillée du document

28 mars 2002 version initiale.