

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur Cisco Unified Call Manager

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-2006-AVI-293>

Gestion du document

Référence	CERTA-2006-AVI-293
Titre	Multiples vulnérabilités sur Cisco Unified Call Manager
Date de la première version	13 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Exécution de code arbitraire ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Unified Call Manager version 5.0(1) ;
- Cisco Unified Call Manager version 5.0(2) ;
- Cisco Unified Call Manager version 5.0(3) ;
- Cisco Unified Call Manager version 5.0(3a) ;

3 Résumé

Plusieurs vulnérabilités présentes dans Cisco Unified Call Manager (CUCM) sur l'interface en ligne de commande et sur le protocole SIP peuvent être exploitées par un utilisateur mal intentionné pour exécuter du code arbitraire avec les privilèges administrateur ou réaliser un déni de service sur l'équipement vulnérable.

4 Description

CUCM est l'application Cisco en charge du traitement des appels sur un réseau VOIP.

Plusieurs vulnérabilités sont présentes sur Cisco Unified Call Manager (CUCM) :

- Deux vulnérabilités sont présentes dans le traitement de certaines commandes de l'interface en ligne de commande (CLI) qui permet d'administrer cet équipement. La première vulnérabilité permet à un utilisateur déjà connecté sur l'interface avec les privilèges administrateur d'exécuter des commandes arbitraires sur le système. La seconde vulnérabilité permet de rediriger n'importe quelle commande vers un répertoire précisé dans la ligne de commande.
- Une autre vulnérabilité de type débordement de mémoire est présente dans le traitement des requêtes SIP. Cette vulnérabilité peut être utilisée par un utilisateur distant mal intentionné afin de réaliser un déni de service ou d'exécuter du code arbitraire sur l'équipement vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco ID 20060712-cucm du 12 juillet 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060712-cucm.shtml>

Gestion détaillée du document

13 juillet 2006 version initiale.