

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco 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-041>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2006-AVI-041 |
| Titre | Multiples vulnérabilités dans Cisco Call Manager |
| Date de la première version | 20 janvier 2006 |
| Date de la dernière version | – |
| Source(s) | Bulletins de sécurité Cisco numéros 68791 et 68792 |
| 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 à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Call Manager version 3.2 et versions antérieures ;
- Cisco Call Manager version 3.3 et versions antérieures à la 3.3(5)SR1a ;
- Cisco Call Manager version 4.0 et versions antérieures à la 4.0(2a)SR2c ;
- Cisco Call Manager version 4.1 et versions antérieures à la 4.1(3)SR2;

3 Résumé

Trois vulnérabilités ont été identifiées dans le Cisco Call Manager. L'exploitation réussie d'une de ces deux vulnérabilités permet de réaliser un déni de service à distance ou une élévation de privilège en local.

4 Description

Trois vulnérabilités ont été découvertes dans le logiciel Cisco Call Manager :

- La première résulte d'une erreur au niveau de la gestion des connexions à destination du port 2000/TCP. Elle peut être exploitée par un utilisateur mal intentionné afin d'utiliser la mémoire de manière abusive et donc provoquer un déni de service.
- La deuxième résulte d'une erreur dans la gestion des connexions à destination des ports 2001/TCP, 2002/TCP et 7727/TCP. Cette vulnérabilité peut être exploitée par des utilisateurs mal intentionnés afin de provoquer le redémarrage de l'équipement vulnérable.
- La troisième résulte d'une erreur présente au niveau de l'interface CCMAAdmin et peut être exploitée par un utilisateur mal intentionné dans le but d'élever ses privilèges (obtention du droit de création, suppression, modification de la configuration des périphériques).

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 XXXXX du 18 janvier 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>
- Bulletin de sécurité Cisco ID XXXXX du 18 janvier 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmpe.shtml>

Gestion détaillée du document

20 janvier 2006 version initiale.