

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Unified Communications 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-2007-AVI-304>

Gestion du document

Référence	CERTA-2007-AVI-304
Titre	Vulnérabilité dans Cisco Unified Communications Manager
Date de la première version	12 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #92015 du 11 juillet 2007
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 à distance ;
- déni de service.

2 Systèmes affectés

- Cisco Unified CallManager versions 3.3(5)SR3 et antérieures ;
- Cisco Unified CallManager versions 4.1(3)SR5 et antérieures ;
- Cisco Unified CallManager versions 4.2(3)SR2 et antérieures ;
- Cisco Unified CallManager version 5.0 ;
- Cisco Unified Communications Manager versions 4.3(1)SR1 et antérieures ;
- Cisco Unified Communications Manager versions 5.1(2) et antérieures.

3 Résumé

Une vulnérabilité dans les logiciels Cisco Unified CallManager et Cisco Unified Communications Manager permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Deux composants de Cisco Unified CallManager et Cisco Unified Communications Manager comportent des failles de type débordement de mémoire : CTL (Certificate Trust List et RIS (Real-Time Information Server). Ces vulnérabilités permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

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 92015 du 11 juillet 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070711-cucm.shtml>

Gestion détaillée du document

12 juillet 2007 version initiale.