

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de 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-2009-AVI-357>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-357                                       |
| Titre                       | Vulnérabilités de Cisco Unified Communications Manager   |
| Date de la première version | 27 août 2009   |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité Cisco 20090826-cucm du 26 août 2009 |
| 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.

## 2 Systèmes affectés

Cisco Unified Communications Manager versions 4.x, 5.x, 6.x et 7.x.

## 3 Résumé

Plusieurs vulnérabilités de Cisco Unified Communications Manager permettent à un utilisateur malveillant de réaliser un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités de Cisco Unified Communications Manager ont été publiées et corrigées :

- le traitement défectueux des paquets SIP malformés, émis vers les ports 5060 et 5061, en UDP comme en TCP, conduit à l'arrêt d'un processus essentiel du système. Le service de transport de la voix est interrompu ;

- le suivi des connexions TCP par le pare-feu intégré au système d'exploitation est vulnérable à une attaque par saturation d'une table du système ;
- les processus de gestion des protocoles SIP (ports 5060 et 5061) et SCCP (ports 2000 et 2443) en TCP sont vulnérables à une attaque épuisant les ressources du système en descripteurs de fichiers. L'exploitation de cette vulnérabilité rend impossible la création de nouvelles connexions.

## 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 20090826-cucm du 26 août 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml>
- Référence CVE CVE-2009-2050 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2050>
- Référence CVE CVE-2009-2051 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2051>
- Référence CVE CVE-2009-2052 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2052>
- Référence CVE CVE-2009-2053 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2053>
- Référence CVE CVE-2009-2054 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2054>

## Gestion détaillée du document

**27 août 2009** version initiale.