

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco Unified

---

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-2012-AVI-530>

---

### Gestion du document

Référence	CERTA-2012-AVI-530
Titre	Vulnérabilité dans Cisco Unified
Date de la première version	27 septembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20120926-cucm du 26 septembre 2012
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 versions 9.x
- Cisco Unified versions 8.x
- Cisco Unified versions 7.x

## 3 Résumé

Une vulnérabilité a été corrigée dans *Cisco Unified*. Elle concerne le protocole *Session Initialisation Protocol* (SIP) utilisé en voie sur IP lors de l'envoi d'un message *Session Description Protocol* (SDP) spécialement conçu.

## 4 Solution

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

## **5 Documentation**

- Bulletin de sécurité Cisco 20120926-cucm du 26 septembre 2012 :  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm>
- Référence CVE CVE-20AA-3949 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20AA-3949>

### **Gestion détaillée du document**

**27 septembre 2012** version initiale.