

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2012-AVI-106>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2012-AVI-106 |
| Titre | Vulnérabilités dans Cisco Unified Communications Manager |
| Date de la première version | 01 mars 2012 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Cisco 20120229-cucm du 29 février 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 Risques

- Exécution de commandes SQL à distance ;
- déni de service à distance.

2 Systèmes affectés

- Cisco Unified Communications Manager Software versions 6.x ;
- Cisco Unified Communications Manager Software versions 7.x ;
- Cisco Unified Communications Manager Software versions 8.x ;
- Cisco Business Edition 3000 ;
- Cisco Business Edition 5000 ;
- Cisco Business Edition 6000.

3 Résumé

Des vulnérabilités dans *Cisco Unified Communications Manager* permettent de réaliser un déni de service et d'exécuter des commandes SQL à distance.

4 Description

Des vulnérabilités ont été découvertes dans *Cisco Unified Communications Manager* :

- des messages SCCP (*Skinny Client Control Protocol*) spécifiques peuvent provoquer le redémarrage de *Cisco Unified Communications Manager* (CVE-2011-4486) ;
- des messages SCCP spécifiques permettent l'exécution de commandes SQL (CVE-2011-4487).

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 20120229-cucm du 29 février 2012 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-cucm>
- Référence CVE CVE-2011-4486 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4486>
- Référence CVE CVE-2011-4487 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4487>

Gestion détaillée du document

01 mars 2012 version initiale.