

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2011-AVI-263>

Gestion du document

Référence	CERTA-2011-AVI-263
Titre	Multiples vulnérabilités dans Cisco Unified Communications Manager
Date de la première version	28 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20110427-cucm du 27 avril 2011
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 ;
- dépôt de fichier ;
- injection SQL.

2 Systèmes affectés

Cisco Unified Communications Manager versions 6.x, 7.x et 8.x.

3 Résumé

De multiples vulnérabilités dans *Cisco Unified Communications Manager* permettent des injections SQL, des dénis de service à distance ou le dépôt d'un fichier.

4 Description

De multiples vulnérabilités ont été découvertes dans *Cisco Unified Communications Manager* :

- trois failles liées au traitement des messages SIP permettent de réaliser un déni de service à distance (CVE-2011-1604, CVE-2011-1605 et CVE-2011-1606) ;

- un utilisateur authentifié qui parvient à intercepter le trafic réseau peut déposer un fichier malveillant sur le système (CVE-2011-1607) ;
- des injections SQL sont possibles, ce qui permet la modification de la configuration du système, ainsi que l'ajout ou la suppression d'utilisateurs. L'une de ces deux vulnérabilités nécessite une authentification préalable (CVE-2011-1609 et CVE-2011-1610).

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 20110427-cucm du 27 avril 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20110427-cucm.shtml>
- Référence CVE CVE-2011-1604 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1604>
- Référence CVE CVE-2011-1605 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1605>
- Référence CVE CVE-2011-1606 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1606>
- Référence CVE CVE-2011-1607 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1607>
- Référence CVE CVE-2011-1609 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1609>
- Référence CVE CVE-2011-1610 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1610>

Gestion détaillée du document

28 avril 2011 version initiale.