



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 16 mars 2009
N° CERTA-2009-AVI-095

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-2009-AVI-095>

Gestion du document

Référence	CERTA-2009-AVI-095
Titre	Vulnérabilité dans Cisco Unified Communications Manager
Date de la première version	16 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20090311-cucmpab du 11 mars 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco Unified CallManager versions 4.1 ;
- Cisco Unified Communications Manager versions 4.2 antérieures à 4.2(3)SR4b ;
- Cisco Unified Communications Manager versions 4.3 antérieures à 4.3(2)SR1b ;
- Cisco Unified Communications Manager versions 5.x antérieures à 5.1(3e) ;
- Cisco Unified Communications Manager versions 6.x antérieures à 6.1(3) ;
- Cisco Unified Communications Manager versions 7.0 antérieures à 7.0(2).

3 Résumé

Une vulnérabilité dans *Cisco Unified Communications Manager* permet d'accéder à un compte d'administration de l'application.

4 Description

Une vulnérabilité a été découverte dans le mécanisme de synchronisation des carnets d'adresses (*Personal Address Book* - PAB) dans *Cisco Unified Communications Manager* (autrefois appelé *CallManager*). Lorsqu'un client de synchronisation PAB s'authentifie auprès d'un serveur *Cisco Unified Communications Manager* (via une connexion HTTPS), des identifiants d'un compte d'administration sont renvoyés « en clair ». Un attaquant peut intercepter ces identifiants.

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 20090311-cucmpab du 11 mars 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090311-cucmpab.shtml>
- Référence CVE-2009-0632 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0632>

Gestion détaillée du document

16 mars 2009 version initiale.