

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco Unified Communications Manager Express

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-2010-AVI-134>

Gestion du document

Référence	CERTA-2010-AVI-134
Titre	Vulnérabilités dans Cisco Unified Communications Manager Express
Date de la première version	25 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20100324-cucme du 24 mars 2010
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

Appareils *Cisco IOS* (incluant *Cisco Unified Communications 500 Series*) configurés pour les fonctionnalités *Cisco Unified CME* ou *Cisco Unified SRST*.

Une liste plus détaillée des systèmes affectés est disponible dans l'avis de l'éditeur.

3 Résumé

Deux vulnérabilités dans *Cisco Unified Communications Manager Express* (CME) permettent de réaliser un déni de service à distance.

4 Description

Deux vulnérabilités ont été découvertes dans *Cisco Unified Communications Manager Express*. Une personne malintentionnée peut, à l'aide de paquets SCCP spécifiques, provoquer un redémarrage du matériel à distance. L'attaque nécessite d'avoir enregistré auprès de l'appareil ciblé l'adresse IP du téléphone de l'attaquant. Toutefois, si la

fonctionnalité d'enregistrement automatique est activée (ce qui est le cas par défaut), l'attaque peut immédiatement suivre l'enregistrement de l'adresse IP.

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 20100324-cucme du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-cucme.shtml>
- Référence CVE CVE-2010-0585 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0585>
- Référence CVE CVE-2010-0586 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0586>

Gestion détaillée du document

25 mars 2010 version initiale.