



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 octobre 2007  
N° CERTA-2007-AVI-441

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco Wireless Control System (WCS)

---

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-2007-AVI-441>

---

### Gestion du document

Référence	CERTA-2007-AVI-441
Titre	Vulnérabilité dans Cisco Wireless Control System (WCS)
Date de la première version	17 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco SA-20071010-WCS du 10 octobre 2007
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

Tous les Cisco WCS convertis à partir de l'utilitaire de conversion CiscoWorks WLSE version 4.1.91.0 et les versions antérieures.

## 3 Résumé

Une vulnérabilité dans l'utilitaire de conversion d'un CiscoWorks WLSE en un Cisco WCS permettrait à un individu malveillant de contourner le politique de sécurité.

## 4 Description

Une vulnérabilité dans l'utilitaire de conversion d'un CiscoWorks Wireless Solution Engine (WLSE) en un Cisco WCS permet à un attaquant de prendre le contrôle du Cisco WCS avec les droits d'administration après conversion. Cet utilitaire créé et utilise par défaut un compte avec des droits d'administration. L'absence

d'obligation de modification de ce compte pendant le processus de conversion permettrait à un attaquant de prendre pleinement le contrôle du système après la conversion.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Cisco SA-20071010-WCS du 10 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20071010-wcs.shtml>
- Référence CVE CVE-2007-5382 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5382>

## **Gestion détaillée du document**

**17 octobre 2007** version initiale.