Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 février 2009
N° CERTA-2009-AVI-051

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les Cisco Wireless LAN Controllers

Gestion du document

Référence	CERTA-2009-AVI-051
Titre	Multiples vulnérabilités dans les Cisco Wireless LAN Controllers
Date de la première version	06 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 108336 du 04 février 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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco 4400 Series Wireless LAN Controllers (WLC) ;
- Cisco Catalyst 6500 Series et 7600 Series Wireless LAN Module (MiSM) ;
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les éléments d'interfaces sans-fil Cisco Wireless LAN Controllers (WLC). L'exploitation de ces dernières peut provoquer l'interruption du service sans-fil ou le redémarrage de l'équipement. Une élévation de privilèges serait possible sous certaines conditions.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les éléments d'interfaces sans-fil Cisco Wireless LAN Controllers (WLC). Ces éléments apportent au système des fonctions nécessaires au fonctionnement du réseau sans-fil et à sa sécurité.

Les vulnérabilités peuvent être exploitées via des trames spécialement construites émises dans les airs. Il est alors possible pour une personne malveillante distante de perturber le système, voire de le forcer à redémarrer. Sous certaines conditions, l'exploitation peut également conduire, selon Cisco, à une élévation de privilèges (pour les WLC de version 4.2.173.0).

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 20090204-wlc du 04 février 2009 :
  http://www.cisco.com/warp/public/707/cisco-sa-20090204-wlc.shtml

Gestion détaillée du document

06 février 2009 version initiale.