

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco Wireless Lan Controllers

---

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-262>

---

### Gestion du document

Référence	CERTA-2011-AVI-262
Titre	Vulnérabilité dans Cisco Wireless Lan Controllers
Date de la première version	28 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20110427-wlc 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.

## 2 Systèmes affectés

- Cisco 2100 Series Wireless LAN Controllers ;
- Cisco WLC526 Mobility Express Controller (AIR-WLC526-K9) ;
- Cisco NME-AIR-WLC Modules for Integrated Services Routers (ISRs) ;
- Cisco NM-AIR-WLC Modules for Integrated Services Routers (ISRs) .

## 3 Résumé

Une vulnérabilité permettant à un utilisateur malintentionné d'effectuer un déni de service a été découverte dans *Cisco Wireless Lan Controllers*.

## 4 Description

Une vulnérabilité a été découverte dans *Cisco Wireless Lan Controllers*. Elle permet à un personne malintentionnée d'effectuer un déni de service via l'envoi d'une série de paquets ICMP.

## **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-wlc du 28 avril 2011 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20110427-wlc.shtml>
- Référence CVE CVE-2011-1613 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1613>

## **Gestion détaillée du document**

**28 avril 2011** version initiale.