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 avril 2007
N° CERTA-2007-AVI-172-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilités dans des produits sans-fil Cisco**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2007-AVI-172-001 |
| Titre | Vulnérabilités dans des produits sans-fil Cisco |
| Date de la première version | 13 avril 2007 |
| Date de la dernière version | 17 avril 2007 |
| Source(s) | Avis de sécurité de CISO du 12 avril 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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- l'application Cisco Wireless LAN Controller (WLC) pour les versions antérieures à 4.0 et 3.2 (incluses) ;
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Wireless LAN Controller Module
- Cisco Catalyst 6500 Series Wireless Service Module (WiSM)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers
- Cisco Aironet 1000 Series
- Cisco Aironet 1500 Series
- l'application Cisco Wireless Control System (WCS) pour les versions antérieures à 4.0.96.0 (incluse) ;

# 3 Résumé

De multiples vulnérabilités ont été identifiées dans deux applications utilisées avec des produits sans-fil Cisco : le Cisco Wireless LAN Controller (`WLC`) et le Cisco Wireless Control System (`WCS`). Les conséquences de l'exploitation de celles-ci sont variées, incluant un déni de service du point d'accès, un accès illégitime à la configuration (lecture et écriture), ou une élévation de privilèges.

# 4 Description

De multiples vulnérabilités ont été identifiées dans deux applications utilisées avec des produits sans-fil Cisco : le Cisco Wireless LAN Controller (`WLC`) et le Cisco Wireless Control System (`WCS`).

Cisco Wireless LAN Controller (`WLC`) est une application qui permet d'administrer les points d'accès Cisco (Aironet), par le biais du protocole `LWAPP` (pour *Lightweight Access Point Protocol*. Parmi les vulnérabilités :

- les paramètres de connexion SNMP sont les valeurs connues `public` et `private`. Cette vulnérabilité permet donc à une personne malveillante distante d'utiliser ces paramètres pour lire et modifier la configuration de `WLC` via SNMP.
- le NPU (`Network Processing Unit`) de `WLC` ne manipulerait pas correctement certains paquets (802.11 ou SNAP par exemple), pouvant perturber le fonctionnement du système.
- un compte d'administration serait imposé et non modifiable. Une personne malveillante pourrait donc utiliser ce compte, par un accès physique sur un port console, pour prendre le contrôle total du système.
- les listes de contrôle d'accès ne sont pas maintenues après le redémarrage du système.

Cisco Wireless Control System (`WCS`) fournit à d'autres systèmes Cisco un ensemble d'outils de gestion et d'administration. Parmi les vulnérabilités le concernant :

- un compte FTP serait non modifiable ni désactivable. Une personne malveillante pourrait ainsi accéder à des fichiers arbitraires hébergeant cette application.
- Le système d'authentification permettrait sous certaines conditions à un utilisateur d'élever ses privilèges à ceux de l'administrateur (`SuperUsers`).
- Certaines pages de `WCS` seraient accessibles sans demande de mot de passe, par tout utilisateur, même non authentifié. Cette vulnérabilité permettrait ainsi de récupérer des informations sur la topologie du réseau, la position des points d'accès, etc.

# 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 ID 82129 du 12 avril 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070412-wlc.shtml
- Bulletin de sécurité Cisco ID 82128 du 12 avril 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070412-wcs.shtml
- Référence CVE CVE-2007-2032 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2032
- Référence CVE CVE-2007-2033 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2033
- Référence CVE CVE-2007-2034 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2034
- Référence CVE CVE-2007-2035 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2035
- Référence CVE CVE-2007-2036 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2036
- Référence CVE CVE-2007-2037 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2037

- Référence CVE CVE-2007-2038 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2038
- Référence CVE CVE-2007-2039 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2039
- Référence CVE CVE-2007-2040 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2040
- Référence CVE CVE-2007-2041 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2041

## Gestion détaillée du document

**13 avril 2007** version initiale.
**17 avril 2007** ajout des références CVE.