Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 mars 2012
N° CERTA-2012-AVI-107

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Wireless LAN Controllers

Gestion du document

Référence	CERTA-2012-AVI-107
Titre	Multiples vulnérabilités dans Cisco Wireless LAN Controllers
Date de la première version	01 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20120229-wlc du 29 février 2012
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

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

2 Systèmes affectés

- *Cisco 2000 Series WLC* ;
- *Cisco 2100 Series WLC* ;
- *Cisco 2500 Series WLC* ;
- *Cisco 4100 Series WLC* ;
- *Cisco 4400 Series WLC* ;
- *Cisco 5500 Series WLC* ;
- *Cisco 500 Series Wireless Express Mobility Controllers* ;
- *Cisco Wireless Services Modules* (WISM) ;
- *Cisco Wireless Services Modules* version 2 (WSIM version 2) ;
- *Cisco NME-AIR-WLC Modules for Integrated Services Routers* ;

- *Cisco NM-AIR-WLC Modules for Integrated Services Routers* ;
- *Cisco Catalyst 3750G Integrated WLCs* ;
- *Cisco Flex 7500 Series Cloud Controllers*.

3 Résumé

De multiples vulnérabilités dans *Cisco Wireless LAN Controllers* permettent de réaliser des dénis de service à distance et de modifier la configuration du matériel.

4 Description

De multiples vulnérabilités ont été découvertes dans *Cisco Wireless LAN Controllers* :

- un attaquant distant peut, sans authentification, provoquer un arrêt inopiné du matériel en soumettant une URL mal formée à l'interface de gestion (CVE-2012-0368) ;
- un attaquant distant peut, sans authentification, provoquer un redémarrage du matériel en envoyant une série de paquets IPv6 (CVE-2012-0369) ;
- un attaquant distant peut, sans authentification, provoquer un redémarrage du matériel en envoyant une série de paquets HTTP ou HTTPS (CVE-2012-0370) ;
- un attaquant distant peut, dans certains cas, se connecter sans authentification au contrôleur via le port 1023/tcp et en modifier la configuration. Cette vulnérabilité n'affecte que *Cisco 4400 Series WLC*, *WISM* (version 1) et *Cisco Catalyst 3750G Integrated WLCs* (CVE-2012-0371).

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 20120229-wlc du 29 février 2012 :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-wlc
- Référence CVE CVE-2012-0368 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0368
- Référence CVE CVE-2012-0369 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0369
- Référence CVE CVE-2012-0370 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0370
- Référence CVE CVE-2012-0371 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0371

Gestion détaillée du document

01 mars 2012 version initiale.