Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2007
N° CERTA-2007-AVI-335

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans certains produits sans-fil Cisco

Gestion du document

Référence	CERTA-2007-AVI-335
Titre	Multiples vulnérabilités dans certains produits sans-fil Cisco
Date de la première version	27 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #97823 du 24 juillet 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.

2 Systèmes affectés

- Cisco 4400 Series Wireless LAN Controllers ;
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers ;
- Cisco Calalyst 6500 Series Wireless Service Module (WiSM).

3 Résumé

De multiples vulnérabilités sont présentes dans des équipements sans-fil de Cisco et permettent de provoquer un déni de service à distance.

4 Description

Trois vulnérabilités sont présentes dans les produits sans-fil de Cisco :

- une première faille est relative à la manière dont ces équipements gèrent les requêtes ARP (Address Resolution Protocol) de type unicast ;

- une deuxième concerne la façon dont est mise en œuvre la gestion des paquets de diffusion (`Broadcast`) à destination d'un client déjà connu ;
- une dernière vulnérabilité concerne la façon dont est géré le nomadisme (`roaming`) de clients entre différents `LAN Controllers Cisco`.

Pour chacune de ces vulnérabilités, un utilisateur distant mais connecté sur le réseau sans-fil peut provoquer un déni de service.

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 97823 du 24 juillet 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070724-arp.shtml
- Référence CVE CVE-2007-4011 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4011
- Référence CVE CVE-2007-4012 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4012

Gestion détaillée du document

27 juillet 2007 version initiale.