



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2009
N° CERTA-2009-AVI-301

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco WLC

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-2009-AVI-301>

Gestion du document

Référence	CERTA-2009-AVI-301
Titre	Multiples vulnérabilités dans Cisco WLC
Date de la première version	29 juillet 2009
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco cisco-sa-20090727-wlc du 27 juillet 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.

2 Systèmes affectés

Les systèmes déployant Cisco Wireless LAN Controllers (WLC) dont :

- Cisco 1500 Series ;
- Cisco 2000 Series ;
- Cisco 2100 Series ;
- Cisco 4100 Series ;
- Cisco 4200 Series ;
- Cisco 4400 Series ;
- Cisco Wireless Services Modules (WiSM) ;
- Cisco WLC Modules ;
- Cisco Catalyst 3750G Integrated WLC.

Les produits Cisco Wireless Controller 5500 Series ne sont pas affectés.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le système de gestion de connexion sans-fil Cisco Wireless LAN Controller (WLC). L'exploitation de ces dernières peut être effectuée à distance, par le biais de trames spécialement construites, afin de perturber le système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le système de gestion de connexion sans-fil Cisco Wireless LAN Controller (WLC). Il ne manipulerait pas correctement certaines trames HTTP, HTTPS ou SSH, en particulier des requêtes ou des requêtes d'authentification. Ces vulnérabilités peuvent être exploitées à distance par une personne malveillante afin de perturber le fonctionnement du 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 20090727-wlc du 27 juillet 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090727-wlc.shtml>
- Référence CVE CVE-2009-1164 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1164>
- Référence CVE CVE-2009-1165 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1165>
- Référence CVE CVE-2009-1166 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1166>
- Référence CVE CVE-2009-1167 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1167>

Gestion détaillée du document

29 juillet 2009 version initiale.