



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 novembre 2005
N° CERTA-2005-AVI-432

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de certains équipements de réseau sans-fil de Cisco

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-2005-AVI-432>

Gestion du document

Référence	CERTA-2005-AVI-432
Titre	Vulnérabilité de certains équipements de réseau sans-fil de Cisco
Date de la première version	03 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #20051102-lwapp du 02 novembre 2005
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- La série Cisco 2000 Wireless LAN controller ;
- La série Cisco 2400 Wireless LAN controller ;
- La série Cisco Aironet 1130 AG Access Point ;
- La série Cisco Aironet 1200 Access Point ;
- La série Cisco Aironet 1240 AG Access Point.

3 Résumé

Une vulnérabilité dans certains équipements de réseau sans-fil Cisco permet à un utilisateur distant de contourner la politique de sécurité du système.

4 Description

Une faiblesse dans la mise en œuvre du LWAPP (LightWeight Access Point Protocol) des Wireless LAN controller Cisco fait que ces derniers peuvent accepter du trafic en clair provenant d'un client arbitraire alors qu'il sont configurés pour n'autoriser que du trafic chiffré. Ceci permet à un utilisateur distant mal intentionné d'injecter du trafic arbitraire dans un réseau chiffré sans authentification préalable.

Remarque : La vulnérabilité n'est exploitable que si le point d'accès ou *Access Point* utilise LWAPP et est contrôlé par un Wireless LAN Controller séparé. Elle n'est pas applicable à un point d'accès autonome.

5 Solution

Se référer au bulletin de sécurité Cisco pour appliquer le correctif approprié (cf. Documentation).

6 Documentation

- Site de l'éditeur :
<http://www.cisco.com>
- Bulletin de sécurité Cisco #20051102-lwapp du 02 novembre 2005 :
<http://www.cisco.com/warp/public/707/cisco-sa-20051102-lwapp.shtml>

Gestion détaillée du document

03 novembre 2005 version initiale.