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 juin 2006
N° CERTA-2006-AVI-264

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans plusieurs produits sans fil de CISCO

Gestion du document

Référence	CERTA-2006-AVI-264
Titre	Vulnérabilités dans plusieurs produits sans fil de CISCO
Date de la première version	29 juin 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité CISCO
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Wireless Access point and Wireless Bridge 350 ;
- Wireless Access point 1100 ;
- Wireless Access point 1130 ;
- Wireless Access point 1200 ;
- Wireless Access point 1240 ;
- Wireless Access point 1310 ;
- Wireless Access point 1410 ;
- Cisco Wireless Control System (WCS) 3.2 ;
- Cisco Wireless Control System (WCS) 4.0 ;

3 Résumé

Plusieurs vulnérabilités sont présentes sur deux logiciels wifi de CISCO. Ces vulnérabilités peuvent être utilisées pour contourner l'authentification et élever ses privilèges sur le système.

4 Description

- Une première vulnérabilité est présente sur l'interface web du point d'acces wifi Cisco. Cette vulnérabilité permet à un utilisateur mal intentionné de contourner l'authentification et d'obtenir les privilèges de l'administrateur sur le point d'accès.
- D'autres vulnérabilités sont présentes sur `Cisco Wireless Control System (WCS)`. Ces vulnérabilités permettent à un utilisateur mal intentionné d'accéder à des informations sensibles, de s'authentifier via un mot de passe administrateur par défaut, de réaliser une attaque de type « Cross Site Scripting » ou encore de lire et d'écrire des fichiers sur WCS.

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 20060628-ap du 28 juin 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060628-ap.shtml
- Bulletin de sécurité Cisco ID 20060628-wcs du 28 juin 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060628-wsc.shtml
- Référence CVE CAN-2006-3226 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-3226

Gestion détaillée du document

29 juin 2006 version initiale.