Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 novembre 2006
N° CERTA-2006-AVI-490

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des pilotes pour les puces Wi-Fi Broadcom

Gestion du document

Référence	CERTA-2006-AVI-490
Titre	Vulnérabilités des pilotes pour les puces Wi-Fi Broadcom
Date de la première version	13 novembre 2006
Date de la dernière version	–
Source(s)	Annonce du "Month of Kernel Bugs" MoKB-11-11-2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Le pilote Broadcom BCMWL5.SYS, pour la version 3.50.21.10 ;
- Le pilote Linksys WPC300N *Wireless-N Notebook Adapter*, pour les versions antérieures à 4.80.28.7.

Cette liste n'est pas définitive. Plusieurs fabriquants utilisent également cette puce dans leur matériel, et possèdent des pilotes particuliers, dérivés du BCMWL5.SYS.

3 Description

Une vulnérabilité a été identifiée dans certains pilotes pour les produits Wi-Fi contenant des puces Broadcom. Ils ne manipuleraient pas correctement certains paquets répondant à une requête de sondage (*Probe Request*), avec un identifiant SSID de longueur trop importante.

Une personne pourrait profiter de cette vulnérabilité, pour envoyer des paquets de réponse malformés, afin d'exécuter du code arbitraire à distance sur la machine. Les solutions de sécurité associées à la connexion Wi-Fi (WPA, VPN, etc.) ne protègent pas contre de telles attaques qui opèrent à une couche protocolaire plus basse.

Le pilote Broadcom développé pour le système d'exploitation Microsoft Windows se nomme `BCMWL5.SYS`. Cependant, certains constructeurs modifient les pilotes qui sont fournis avec leurs machines. Chacun doit donc mettre à jour sa propre version, en tenant compte des corrections faites par Broadcom. Les mises à jour des constructeurs ne sont pas nécessairement automatiques.

4 Solution

Se référer au bulletin de sécurité des différents éditeurs pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Mise à jour Linksys pour WPC300N (*Wireless-N Notebook Adapter*) du 07 novembre 2006 :
  http://www-fr.linksys.com
- Avis du site *Month of Kernel Bugs* MoKB-11-11-2006 :
  http://projects.info-pull.com/mokb/MOKB-11-11-2006.html
- Site officiel de Broadcom, et accès aux pilotes :
  http://www.broadcom.com/support/

Gestion détaillée du document

13 novembre 2006 version initiale.