Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 août 2007
N° CERTA-2007-AVI-372

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des pilotes WiFi Atheros pour Windows

Gestion du document

Référence	CERTA-2007-AVI-372
Titre	Vulnérabilités des pilotes WiFi Atheros pour Windows
Date de la première version	22 août 2007
Date de la dernière version	–
Source(s)	Avis de sécurité WVE-2007-0012 de WVE publiée le 21 août 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

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

2 Systèmes affectés

- les versions des pilotes Atheros antérieures à 5.3.0.35 et 6.0.3.67.

Plusieurs vendeurs matériels utilisent des versions de ces pilotes adaptées pour leurs produits. Leur numérotation de versions peut donc être différente de celle d'origine.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les pilotes WiFi Atheros pour Windows. Elles permettraient à une personne distante de perturber le système, ou d'exécuter des commandes arbitraires, par le simple envoi de trames WiFi spécialement construites.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les pilotes WiFi Atheros pour Windows. Ces derniers ne manipuleraient pas correctement des trames ayant un champ `IE` (pour *Information Element*) malformé, incluant les balises et les réponses à un sondage (`probe`).

Ces vulnérabilités peuvent être exploitées par une personne malveillante distante, par la simple émission de trames WiFi spécialement construites. Les conséquences seraient alors la perturbation ou l'exécution de code arbitraire avec des privilèges élevés sur le système vulnérable.

Les mesures de protection telles que le WEP, le WPA ou le WPA2 (802.11i) ne protègent pas contre de telles vulnérabilités.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site officiel d'Atheros :
  http://www.atheros.com
- Référence CVE CVE-2007-2927 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2927
- Avis de sécurité WVE-2007-0012 du 21 août 2007 :
  http://www.wirelessve.org/entries/show/WVE-2007-0012
- Avis de sécurité US-CERT VU#730169 du 14 août 2007 :
  http://www.kb.cert.org/vuls/id/730169

Gestion détaillée du document

22 août 2007 version initiale.