



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 mai 2007
N° CERTA-2007-AVI-223

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les pilotes sans-fil MadWifi

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-2007-AVI-223>

Gestion du document

Référence	CERTA-2007-AVI-223
Titre	Vulnérabilités dans les pilotes sans-fil MadWifi
Date de la première version	24 mai 2007
Date de la dernière version	–
Source(s)	Tickets de sécurité du site MadWiFi 1270, 1334 et 1335
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.

2 Systèmes affectés

MadWiFi, pour les versions antérieures à 0.9.3.1.

3 Résumé

Trois vulnérabilités ont été identifiées dans les pilotes Linux MadWifi utilisés pour certaines interfaces d'accès aux réseaux sans-fil. Deux d'entre elles sont exploitables à distance, par l'émission de trames sans-fil spécialement construites. Les conséquences peuvent être un dysfonctionnement de la fonctionnalité sans-fil ou l'exécution de code arbitraire sur le système vulnérable.

4 Description

Trois vulnérabilités ont été identifiées dans les pilotes Linux MadWifi, utilisés pour certaines interfaces d'accès aux réseaux sans-fil utilisant une puce atheros :

1. la fonction `ath_beacon_config()` pourrait effectuer une division par zéro pour le calcul de la macro `howmany`, sans vérifier la valeur du dénominateur `intval`. Cette vulnérabilité pourrait être exploitée à distance, par une trame Wi-Fi spécialement construite, afin de perturber le système.
2. la fonction `ieee_80211_ioctl_getwmmparams` ne contrôlerait pas correctement un index de tableau. Cette vulnérabilité peut être exploitée par un utilisateur local et ayant des droits limités, afin d'élever ses privilèges ou d'accéder à certaines données de la mémoire.
3. les paquets de type `Fast Frame` (méthode de compression de données, pouvant s'utiliser avec le standard 802.11e associé à la qualité de service) ne sont pas correctement contrôlés. Leur longueur n'est pas vérifiée, et l'interprétation d'un paquet spécialement construit pourrait ainsi rendre le système indisponible.

5 Solution

Se référer aux tickets de sécurité du projet MadWifi pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site du projet MadWifi :
<http://madwifi.org>
- Ticket de sécurité 1270 du projet MadWifi :
<http://madwifi.org/ticket/1270>
- Ticket de sécurité 1334 du projet MadWifi :
<http://madwifi.org/ticket/1334>
- Ticket de sécurité 1335 du projet MadWifi :
<http://madwifi.org/ticket/1335>
- Référence CVE CVE-2007-1270 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1270>
- Référence CVE CVE-2007-1334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1334>
- Référence CVE CVE-2007-1335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1335>

Gestion détaillée du document

24 mai 2007 version initiale.