

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-491>

---

## Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2007-AVI-491                              |
| Titre                       | Vulnérabilité dans les pilotes sans-fil MadWifi |
| Date de la première version | 14 novembre 2007                                |
| Date de la dernière version | –   |
| Source(s)                   | Mise à jour des pilotes MadWifi                 |
| 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

Déni de service à distance.

## 2 Systèmes affectés

Pilotes MadWifi version 0.9.3.2 et versions antérieures.

## 3 Résumé

Une vulnérabilité permettant de réaliser un déni de service a été découverte dans les pilotes MadWifi.

## 4 Description

Une vulnérabilité a été découverte dans les pilotes sans-fil Madwifi. Cette vulnérabilité est due à une mauvaise gestion des paquets contenant un élément *xrates*. Par le biais d'un paquet spécialement construit il est ainsi possible de causer un déni de service sur l'interface sans-fil utilisant le pilote vulnérable.

## 5 Solution

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

## 6 Documentation

- Mise à jour des pilotes MadWifi :  
[http://sourceforge.net/project/shownotes.php?release\\_id=547876](http://sourceforge.net/project/shownotes.php?release_id=547876)
- Bulletin de sécurité Gentoo GLSA-200711-09 du 07 novembre 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200711-09.xml>
- Référence CVE CVE-2007-5448 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5448>

## Gestion détaillée du document

14 novembre 2007 version initiale.