

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Wireshark

---

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-2009-AVI-139>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-139-001   |
| Titre                       | Vulnérabilités dans Wireshark                                    |
| Date de la première version | 14 avril 2009  |
| Date de la dernière version | 11 mai 2009  |
| Source(s)                   | Bulletin de sécurité Wireshark wnpa-sec-2009-02 du 06 avril 2009 |
| 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

- Dénis de service à distance.

## 2 Systèmes affectés

- Les versions de Wireshark antérieures à la 1.0.7.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'outil d'analyse réseau Wireshark. L'exploitation de ces dernières via des trames spécialement construites peut perturber le fonctionnement de l'application.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans l'outil d'analyse réseau Wireshark. Elles concernent en particulier l'interprétation et la manipulation de trames via les modules d'analyse suivants :

- PROFINET ;
- LDAP ;

– CPHAP (*Check Point High-Availability Protocol*).

Une personne malveillante peut exploiter l'une de ces vulnérabilités en construisant des trames adaptées puis en les injectant dans le réseau. L'exploitation perturbe alors le fonctionnement de l'application de capture.

L'ouverture de fichiers au format Tektronix (.rf5) peut également être problématique.

## 5 Solution

Se référer au bulletin de sécurité wnpa-sec-2009-02 de Wireshark pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2009-02 du 06 avril 2009 :  
<http://www.wireshark.org/security/wnpa-sec-2009-02.html>
- Bulletin de sécurité Debian DSA-1785 du 01 mai 2009 :  
<http://www.debian.org/security/2009/dsa-1785>
- Référence CVE CVE-2009-1210 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1210>
- Référence CVE CVE-2009-1267 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1267>
- Référence CVE CVE-2009-1268 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1268>
- Référence CVE CVE-2009-1269 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1269>

## Gestion détaillée du document

**14 avril 2009** version initiale.

**11 mai 2009** ajout de la référence au bulletin de sécurité Debian.