

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-2011-AVI-232>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2011-AVI-232  |
| Titre                       | Vulnérabilités dans Wireshark   |
| Date de la première version | 19 avril 2011   |
| Date de la dernière version | –   |
| Source(s)                   | Bulletins de sécurité wnpa-sec-2011-05 et wnpa-sec-2011-06 du 14 avril 2011 |
| 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

- *Wireshark* versions 1.2.15 et antérieures (branche 1.2.x) ;
- *Wireshark* versions 1.4.4 et antérieures (branche 1.4.x).

## 3 Résumé

Des vulnérabilités dans *Wireshark* permettent de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

Des vulnérabilités ont été découvertes dans *Wireshark*. Elles affectent les analyseurs NFS, X.509if et DECT. L'exploitation de ces failles permet de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

## **5 Solution**

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

## **6 Documentation**

- Bulletins de sécurité Wireshark wnpa-sec-2011-05 et wnpa-sec-2011-06 du 14 avril 2011 :  
<http://www.wireshark.org/security/wnpa-sec-2011-05.html>  
<http://www.wireshark.org/security/wnpa-sec-2011-06.html>

## **Gestion détaillée du document**

**19 avril 2011** version initiale.