

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-325>

---

### Gestion du document

Référence	CERTA-2011-AVI-325
Titre	Vulnérabilités dans Wireshark
Date de la première version	03 juin 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité wnpa-sec-2011-07 et wnpa-sec-2011-08 du 31 mai 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

Déni de service à distance.

## 2 Systèmes affectés

- Wireshark versions 1.2.16 et antérieures (branche 1.2.x) ;
- Wireshark versions 1.4.6 et antérieures (branche 1.4.x).

## 3 Résumé

Des vulnérabilités dans Wireshark permettent de réaliser un déni de service à distance.

## 4 Description

Des vulnérabilités ont été découvertes dans Wireshark. Elles peuvent être exploitées par une personne distante malveillante, à l'aide de fichiers spécialement conçus, pour provoquer un déni de service.

## **5 Solution**

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

## **6 Documentation**

- Bulletins de sécurité wnpa-sec-2011-07 et wnpa-sec-2011-08 du 31 mai 2011 :  
<http://www.wireshark.org/security/wnpa-sec-2011-07.html>  
<http://www.wireshark.org/security/wnpa-sec-2011-08.html>

## **Gestion détaillée du document**

**03 juin 2011** version initiale.