

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans Wireshark

### Gestion du document

Référence	CERTFR-2016-AVI-327
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	05 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2016-56 du 04 octobre 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-57 du 04 octobre 2016
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(s)

- déni de service à distance

### 2 - Systèmes affectés

Wireshark versions 2.2.0 et antérieures

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Wireshark*. Elles permettent à un attaquant de provoquer un déni de service à distance.

### 4 - Solution

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

### 5 - Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2016-56 du 04 octobre 2016  
<https://www.wireshark.org/security/wnpa-sec-2016-56.html>

– Bulletin de sécurité Wireshark wnpa-sec-2016-57 du 04 octobre 2016  
<https://www.wireshark.org/security/wnpa-sec-2016-57.html>

## **Gestion détaillée du document**

**05 octobre 2016** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-327>

---