



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 18 septembre 2009  
N° CERTA-2009-AVI-388

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-388>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-388                         |
| Titre                       | Multiples vulnérabilités dans Wireshark    |
| Date de la première version | 18 septembre 2009                          |
| Date de la dernière version | –  |
| Source(s)                   | Bulletins de sécurité du 15 septembre 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

Déni de service à distance.

## 2 Systèmes affectés

- Wireshark versions 1.0.8 et antérieures ;
- Wireshark versions 1.2.1 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans Wireshark permettent à un utilisateur distant malintentionné de provoquer un déni de service.

## 4 Description

Trois vulnérabilités sont présentes dans Wireshark :

- la première est relative à l'analyseur de protocole *OpcUa* des versions 0.99.6 à 1.0.8 et 1.2.0 à 1.2.1 ;
- la seconde concerne l'analyseur de protocole GSM A RR des versions 1.2.0 et 1.2.1 ;

– la dernière est relative à la mise en œuvre de TLS dans les versions 1.2.0 et 1.2.1.  
Toutes ces vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).  
Les versions 1.0.9 et 1.2.2 de `Wireshark` corrigent le problème :  
<http://www.wireshark.org/download.html>

## 6 Documentation

- Bulletins de sécurité Wireshark du 15 septembre 2009 :  
<http://www.wireshark.org/security/wnpa-sec-2009-05.html>  
<http://www.wireshark.org/security/wnpa-sec-2009-06.html>
- Référence CVE CVE-2009-2562 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2562>
- Référence CVE CVE-2009-2563 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2563>

## Gestion détaillée du document

**18 septembre 2009** version initiale.