

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans OpenAFS

---

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-2007-AVI-142>

---

### Gestion du document

Référence	CERTA-2007-AVI-142
Titre	Vulnérabilités dans OpenAFS
Date de la première version	27 mars 2007
Date de la dernière version	–
Source(s)	Avis de sécurité OpenAFS du 21 mars 2007
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- élévation de privilèges ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- OpenAFS, pour les versions comprises entre 1.0 et 1.4.3 (version incluse) ;
- OpenAFS, pour les versions 1.5.0 à 1.5.16 inclus.

## 3 Description

Une vulnérabilité a été identifiée dans le système de fichiers distribué OpenAFS. Ce dernier fonctionne en mode client-serveur, mais le gestionnaire de cache n'utiliserait pas de connexion authentifiée pour les utilisateurs (clients) qui chercheraient à le contacter. Une personne malveillante pourrait donc accéder à certaines données dans le cache, voire élever ses privilèges en profitant du mode `setuid` utilisé par défaut par l'application.

## **4 Solution**

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

## **5 Documentation**

- Page d'accueil du projet OpenAFS :  
<http://www.openafs.org>
- Avis de sécurité OpenAFS 2007-001 du 21 mars 2007 :  
<http://www.openafs.org/pages/security/OPENAFS-SA-2007-001.txt>
- Référence CVE CVE-2007-1507 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1507>

## **Gestion détaillée du document**

**27 mars 2007** version initiale.