



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 janvier 2009  
N° CERTA-2009-AVI-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans Samba**

---

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-001>

---

### Gestion du document

Référence	CERTA-2009-AVI-001
Titre	Vulnérabilité dans Samba
Date de la première version	05 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Samba CVE-2009-0022
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 la confidentialité des données.

## 2 Systèmes affectés

Samba versions 3.2.0 à 3.2.6.

## 3 Résumé

Une vulnérabilité présente dans le serveur de fichier Samba permet à un utilisateur malintentionné distant de contourner la politique de sécurité du système vulnérable.

## 4 Description

Une vulnérabilité est présente dans le serveur de fichier Samba. Cette vulnérabilité concerne les serveurs configurés avec la directive *registry shares* positionnée à *yes*. Dans ces conditions et avec un certain type de client samba, il est possible à un utilisateur distant malintentionné d'accéder à la racine du système de fichiers ("/") avec les privilèges du compte valide utilisé pour se connecter auprès du serveur Samba vulnérable.

## 5 Solution

La version 3.2.7 corrige le problème :

<http://us6.samba.org/samba/ftp/stable/samba-3.2.7.tar.gz>

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

## 6 Documentation

– Bulletin de sécurité Samba CVE-2009-0022 :

<http://us1.samba.org/samba/security/CVE-2009-0022.html>

– Référence CVE CVE-2009-0022 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0022>

## Gestion détaillée du document

**05 janvier 2009** version initiale.