

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-2010-AVI-038>

---

### Gestion du document

Référence	CERTA-2010-AVI-038
Titre	Vulnérabilité dans Samba
Date de la première version	29 janvier 2010
Date de la dernière version	–
Source(s)	Report de bogue Samba numéro 6853 du 26 janvier 2010 Report de bogue Red Hat numéro 532940 du 28 janvier 2010
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Samba versions 3.x.

## 3 Résumé

Une vulnérabilité permettant l'élévation de privilèges a été découverte dans Samba.

## 4 Description

Une vulnérabilité a été découverte dans Samba. Cette vulnérabilité est due à une erreur dans la gestion de l'utilitaire `mount.cifs`. L'exploitation de cette vulnérabilité permet de contourner la politique de sécurité mise en place et, éventuellement, d'acquies des privilèges plus élevés dans le cas où `mount.cifs` est configuré avec un `suid root`.

## 5 Solution

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

## 6 Documentation

- Report de bogue Samba numéro 6853 du 26 janvier 2010 :  
[http://bugzilla.samba.org/show\\_bug.cgi?id=6853](http://bugzilla.samba.org/show_bug.cgi?id=6853)
- Report de bogue Red Hat numéro 532940 du 28 janvier 2010 :  
[http://bugzilla.redhat.com/show\\_bug.cgi?id=532940](http://bugzilla.redhat.com/show_bug.cgi?id=532940)
- Référence CVE CVE-2009-3297 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3297>

## Gestion détaillée du document

**29 janvier 2010** version initiale.