

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-133>

---

### Gestion du document

Référence	CERTA-2010-AVI-133
Titre	Vulnérabilité dans Samba
Date de la première version	25 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ubuntu USN-918-1 du 24 mars 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

Atteinte à la confidentialité des données.

## 2 Systèmes affectés

Samba versions 3.3.x, 3.4.x et 3.5.x.

## 3 Résumé

Une vulnérabilité dans le serveur Samba donne à un utilisateur distant l'accès en lecture à tous les fichiers du serveurs.

## 4 Description

La configuration par défaut du serveur Samba contient la directive : `wide links = yes`.

Conjuguée aux extensions Unix des clients et à certains droits sur des partages, elle permet à un utilisateur distant d'accéder à tous les fichiers présents sur le serveur.

## 5 Solution

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

## 6 Documentation

- Rapport d'erreur du projet Samba :  
[http://www.samba.org/samba/news/symlink\\_attack.html](http://www.samba.org/samba/news/symlink_attack.html)
- Bulletin de sécurité Ubuntu USN-918-1 du 24 mars 2010 :  
<http://www.ubuntulinux.org/usn/usn-918-1>
- Référence CVE CVE-2010-0926 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0926>

## Gestion détaillée du document

**25 mars 2010** version initiale.