

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-420>

---

### Gestion du document

Référence	CERTA-2009-AVI-420-002
Titre	Multiples vulnérabilités dans Samba
Date de la première version	02 octobre 2009
Date de la dernière version	04 février 2009
Source(s)	Bulletins de sécurité Samba du 01 octobre 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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Samba versions 3.0.36 et antérieures ;
- Samba versions 3.2.14 et antérieures ;
- Samba versions 3.3.7 et antérieures ;
- Samba versions 3.4.2 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans Samba permettent à un utilisateur distant malintentionné de porter atteinte à la confidentialité des données ou de provoquer un déni de service.

## 4 Description

Trois vulnérabilités ont été identifiées dans Samba :

- la première est relative à la fonction *mount.cifs* et permet à un utilisateur distant malintentionné d'obtenir, sous certaines conditions, le contenu de certains fichiers ;
- la seconde est relative à une erreur dans le traitement de certaines requêtes SMB et permet à un utilisateur distant authentifié de provoquer un déni de service ;
- la dernière concerne un problème dans la gestion de certaines entrées dans le fichier */etc/passwd* et permet à un utilisateur distant de porter atteinte à la confidentialité des fichiers du serveur vulnérable.

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité Samba du 01 octobre 2009 :  
<http://www.samba.org/samba/security/CVE-2009-2948.html>  
<http://www.samba.org/samba/security/CVE-2009-2906.html>  
<http://www.samba.org/samba/security/CVE-2009-2813.html>
- Bulletin de sécurité HP c01940841 du 27 janvier 2010 :  
[http://itrc.hp.com/service/cki/docDisplay.do?docId=emr\\_na-c01940841](http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01940841)
- Bulletin de sécurité Sun Solaris du 17 novembre 2009 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-271069-1>
- Référence CVE CVE-2009-2948 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2948>
- Référence CVE CVE-2009-2906 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2906>
- Référence CVE CVE-2009-2813 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2813>

## Gestion détaillée du document

**02 octobre 2009** version initiale ;

**19 novembre 2009** ajout de la référence au bulletin Sun Solaris.

**04 février 2010** ajout de la référence au bulletin HP.