



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 09 juin 2004  
N° CERTA-2004-AVI-038-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le serveur 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-2004-AVI-038>

---

## Gestion du document

Référence	CERTA-2004-AVI-038-002
Titre	Vulnérabilité dans le serveur samba
Date de la première version	13 février 2004
Date de la dernière version	09 juin 2004
Source(s)	Bulletin Samba
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

Accès non autorisé.

## 2 Systèmes affectés

Les versions de samba antérieures à la version 3.0.

## 3 Résumé

Une vulnérabilité a été découverte dans le serveur samba sous linux.

## 4 Description

Samba est un logiciel libre, open source, utilisé pour la mise en œuvre des partages réseau à l'aide des protocoles SMB et CIF sous Unix. Le script `mk smbpasswd . sh` permet d'engendrer les fichiers des mots de passe des utilisateurs samba (`smbpasswd`) à partir du fichier `passwd`. Une vulnérabilité présente dans la création des comptes à l'aide du script `mk smbpasswd . sh` permet à un utilisateur mal intentionné d'accéder à un compte utilisateur légitime sans autorisation.

## 5 Solution

Mettre à jour le logiciel samba avec la version 3.0.2.

Bulletin samba :

- Avis de sécurité Samba :  
<http://www.samba.org/samba/whatsnew/samba-3.0.2.html>
- Avis de sécurité RedHat RHSA-2004:064 du 21 mai 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-064.html>
- Avis de sécurité FreeBSD du 15 avril 2004 :  
<http://www.vuxml.org/freebsd/>

## 6 Documentation

- Référence CVE CAN-2004-0082 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0082>

## Gestion détaillée du document

**13 février 2004** version initiale.

**13 mai 2004** ajout de la référence au bulletin de sécurité FreeBSD.

**09 juin 2004** ajout de la référence au bulletin de sécurité RedHat.