Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 décembre 2002
N° CERTA-2002-AVI-252-003

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité de Samba



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2002-AVI-252-003 |
| Titre | Vulnérabilité de Samba |
| Date de la première version | 25 novembre 2002 |
| Date de la dernière version | 13 decembre 2002 |
| Source(s) | Avis de Sécurité DSA-200 de Debian<br>Avis de Sécurité SuSE-SA:2002:045 de SuSE<br>Avis de Sécurité RHSA-2002:266 de Red Hat |
| 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

Elévation de privilèges.

## 2 Systèmes affectés

- Samba versions 2.2.2 à 2.2.6 ;
- CIFS/9000 Server 2.2 versions A.01.08, A.01.08.01 et A.01.09.

## 3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans le serveur `smbd` permet à un utilisateur mal intentionné de réaliser, sous certaines conditions, une élévation de privilèges.

# 4 Description

Samba est une implémentation du protocole `SMB`.

Une vulnérabilité de type débordement de mémoire est présente dans la routine calculant la longueur utilisée lors de la demande de changement d'un mot de passe réalisée par un client.

L'exploitation de cette vulnérabilité peut permettre à un utilisateur mal intentionné d'exécuter, à distance, du code arbitraire avec les privilèges de l'administrateur système `root`.

# 5 Solution

La version 2.2.7 de Samba corrige cette vulnérabilité.

# 6 Documentation

- Site de Samba :
  http://www.samba.org
- Bulletin de sécurité RHSA-2002:266 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2002-266.html
- Bulletin de sécurité DSA-200 de Debian :
  http://www.debian.org/security/2002/dsa-200
- Bulletin de sécurité SuSE-SA:2002:045 de SuSE :
  http://www.suse.com/de/security/2002_045_samba.html
- Bulletin de sécurité MDKSA-2002:081 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:081
- Bulletin de sécurité 20021204-01-I de SGI :
  ftp://patches.sgi.com/support/free/security/advisories/20021204-01-I
- Bulletin de sécurité HPSBUX0212-0230 de Hewlett-Packard :
  http://itrc.hp.com

# Gestion détaillée du document

**25 novembre 2002** version initiale.

**27 novembre 2002** ajout de la référence au bulletin de sécurité MDKSA-2002:081 de Mandrake.

**10 décembre 2002** ajout de la référence au bulletin de sécurité 20021204-01-I de SGI.

**13 décembre 2002** ajout de la référence au bulletin de sécurité HPSBUX0212-0230 de Hewlett-Packard.