Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juin 2001
N° CERTA-2001-AVI-069

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans samba

Gestion du document

Référence	CERTA-2001-AVI-069
Titre	Vulnérabilité dans Samba
Date de la première version	27 juin 2001
Date de la dernière version	–
Source(s)	Avis 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

Un utilisateur mal intentionné disposant d'un compte sur le serveur samba peut obtenir les droits administrateurs. Cette vulnérabilité peut également permettre un déni de service.

2 Systèmes affectés

Toutes les versions de samba antérieures à 2.2.0 et 2.0.10 sont vulnérables.

3 Résumé

Une faille dans la gestion du nom des fichiers journaux de samba permet à un utilisateur mal intentionné d'obtenir les droits administrateurs sur la machine. De plus, certains fichiers peuvent être écrasés à distance.

4 Description

Le service samba permet sur UNIX le partage de ressources NETBIOS (protocole SMB). Le fichier de configuration de samba est `/etc/smb.conf`.

Une vulnérabilité existe dans la gestion du nom du fichier de journalisation. Le nom de ce fichier se trouve dans `/etc/smb.conf`.

Cette vulnérabilité peut permettre d'écraser d'autres fichiers et d'obtenir les droits administrateurs pour un utilisateur disposant déjà d'un compte sur la machine.

5 Contournement provisoire

Dans le fichier `/etc/smb.conf`, remplacer toutes les occurences de %m par %I.

6 Solution

Mettre à jour le service samba. Vous trouverez les mises à jour de samba au lien suivant :
http://va.samba.org/samba/ftp/

7 Documentation

http://us1.samba.org/samba/whatsnew/macroexploit.html

Gestion détaillée du document

27 juin 2001 version initiale.