Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mars 2003
N° CERTA-2003-AVI-048-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Samba

Gestion du document

Référence	CERTA-2003-AVI-048-002
Titre	Vulnérabilités de Samba
Date de la première version	17 mars 2003
Date de la dernière version	20 mars 2003
Source(s)	
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de `Samba` des versions 2.0.x à la version 2.2.7a incluse. Pour Debian 3.0 (woody), toutes les versions des paquetages antérieures à la version 2.2.3a-12.1.

3 Résumé

Plusieurs vulnérabilités dans `Samba` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`Samba` est une implémentation du protocole SMB/CIFS (Server Message Block/Common Internet File System). Ce protocole est typiquement utilisé pour partager des fichiers et des imprimantes avec des machines Win-

dows. Plusieurs vulnérabilités dans le démon `smbd` (Server Message Block Daemon) permet à un utilisteur mal intentionné d'exécuter du code arbitraire à distance.

5 Contournement provisoire

- Editer les fichiers `hosts.allow` et `hosts.deny` pour gérer les machines autorisées à utiliser `Samba` ;
- forcer l'écoute du démon seulement sur les interfaces nécessaires ;
- filtrer les ports TCP/139 et TCP/445.

6 Solution

Pour la Debian 3.0 (woody), mettre à jour `Samba` en version 2.2.3a-12.1. Sinon, mettre à jour `Samba` en version 2.2.8.

7 Documentation

- Annonce de la version 2.2.8 par l'equipe Samba :
  http://www.samba.org/samba/whatsnew/samba-2.2.8.html
- Avis de sécurité Debian DSA-262-1 :
  http://www.debian.org/security/2003/dsa-262
- Avis de sécurité Mandrake MDKSA-2003:032 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:032
- Avis de sécurité RedHat RHSA-2003:095-11 :
  https://rhn.redhat.com/errata/RHSA-2003-095.html
- Avis de sécurité Gentoo GLSA:samba (200303-11) :
  http://www.gentoo.org
- Avis de sécurité SuSE SuSE-SA:2003:016 :
  http://www.suse.de/de/security/2003_016_samba.html
- Avis de sécurité SGI Irix :
  http://www.sgi.com/support/security/advisories.html

Gestion détaillée du document

17 mars 2003 version initiale.
18 mars 2003 ajout des bulletins RedHat et Gentoo.
20 mars 2003 ajout des bulletins SuSE et IRIX.