Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mai 2003
N° CERTA-2003-AVI-072-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Samba

Gestion du document

Référence	CERTA-2003-AVI-072-002
Titre	Vulnérabilité sur Samba
Date de la première version	07 avril 2003
Date de la dernière version	22 mai 2003
Source(s)	Liste de diffusion Bugtraq
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 ;
- déni de service.

2 Systèmes affectés

- Les versions antérieures à Samba 2.2.8a et Samba-TNG 0.3.2 ;
- Samba version 2.0.10 et toutes les versions précèdentes.

3 Résumé

Un débordement de pile sur le serveur Samba permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du super utilisateur `root`.

4 Description

Samba est un logiciel libre, open source, utilisé pour fournir une implémentation du protocole `SMB` sur les serveurs Unix.

Un débordement de mémoire présent sur la fonction `trans2.c` utilisée par le démon `smbd` permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

Un outil disponible sur l'Internet permet d'exploiter facilement cette vulnérabilité.

5 Solution

Mettre à jour le serveur samba (cf. section documentation).
Utiliser la dernière version de Samba : Samba 2.2.8a et Samba-TNG 0.3.2.
Une mise à jour est disponible pour les versions 2.0.x.

6 Documentation

- Site internet du logiciel Samba :
  http://www.samba.org
- Site pour le téléchargement des mises à jour et des nouvelles versions :
  http://ftp.easynet.be/samba/ftp/
- Avis de sécurité MDKSA-2003:044 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/
- Avis de sécurité DSA-280-1 de Debian :
  http://www.debian.org/security/2003/dsa-280
- Avis de sécurité SUSE-SA:2003:025 de SuSE :
  http://www.suse.com/de/security/2003_025_samba.html
- Avis de sécurité OpenPKG-SA-2003.028 de OpenPKG :
  http://www.openpkg.org/security/OpenPKG-SA-2003.028-samba.html
- Bulletin de sécurité RHSA-2003:137 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-137.html
- Bulletin de sécurité RHSA-2003:138 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-138.html
- Bulletin de sécurité #53581 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F53581
- Bulletin de sécurité FreeBSD-SN-03:01 de FreeBSD :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SN-03%3A01.asc
- Bulletin de sécurité 20030403-01-P de SGI :
  ftp://patches.sgi.com/support/free/security/advisories/20030403-01-P
- Bulletin de sécurité HPSBUX0304-254 de HP :
  http://itrc.hp.com
- Annonce Apple Mac OS X 10.2.5 :
  http://archives:archives@lists.apple.com/mhonarc/security-announce/msg00028.html
- Référence CVE CAN-2003-00201 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-00201

Gestion détaillée du document

07 avril 2003 version initiale.

08 avril 2003 ajout des avis de sécurité : Mandrake, Debian, SuSE, OpenPKG.

22 mai 2003 ajout des avis de sécurité Red Hat, SUN, SGI, HP, FreeBSD, Apple. Ajout référence CVE.