Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 septembre 2004
N° CERTA-2004-AVI-311-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Samba

Gestion du document

Référence	CERTA-2004-AVI-311-001
Titre	Multiples vulnérabilités de Samba
Date de la première version	14 septembre 2004
Date de la dernière version	23 septembre 2004
Source(s)	Bulletins de sécurité d'iDEFENSE
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

Déni de service.

2 Systèmes affectés

Samba versions 3.0.6 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans Samba permettent à un utilisateur mal intentionné de provoquer un déni de service.

4 Description

Samba est un logiciel libre, open source, utilisé pour la mise en oeuvre des partages réseau à l'aide des protocoles SMB et CIFS sous Unix.

Plusieurs vulnérabilités sont présentes dans samba :

- CVE CAN-2004-0807 : vulnérabilité dans le décodage de données ASN.1 lors de la phase d'authentification d'un utilisateur ;
- CVE CAN-2004-0808 : vulnérabilité dans le traitement de paquets NETBIOS.

L'exploitation de ces vulnérabilités permet à un utilisateur mal intentionné, via l'envoi de paquets habilement constitués, de créer un déni de service en provoquant l'arrêt brutal du service `nmbd` ou la consommation excessive de mémoire par le service `smbd`.

5 Solution

La version 3.0.7 de Samba corrige ces vulnérabilités.

6 Documentation

- Site Internet de Samba :
  http://www.samba.org
- Note "Samba 3.0.x Denial of service flaw" :
  http://sambafr.idealx.org/samba/history/3.0_DOS_sept04_announce.txt
- Bulletin de sécurité "Samba 3.x SMBD remote denial of service vulnerability" d'IDEFENSE :
  http://www.idefense.com/application/poi/display?id=139&type=vulnerabilities
- Bulletin de sécurité "Samba NMBD invalid length denial of service vulnerability" d'IDEFENSE :
  http://www.idefense.com/application/poi/display?id=138&type=vulnerabilities
- Bulletin de sécurité Gentoo GLSA 200409-16 du 13 septembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200409-16.xml
- Bulletin de sécurité Mandrake MDKSA-2004:092 du 13 septembre 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:092
- Bulletin de sécurité FreeBSD "samba3 DoS attack" du 14 septembre 2004 :
  http://www.vuxml.org/freebsd/
- Mise à jour de sécurité du paquetage NetBSD samba :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/samba/README.html
- Bulletin de sécurité Red Har RHSA-2004:467 du 22 septembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-467.html
- Référence CVE CAN-2004-0807 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0807
- Référence CVE CAN-2004-0808 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0808

Gestion détaillée du document

14 septembre 2004 version initiale.
23 septembre 2004 ajout de la référence au bulletin de sécurité de Red Hat.