



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 août 2006  
N° CERTA-2006-AVI-294-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Samba

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-294>

---

### Gestion du document

Référence	CERTA-2006-AVI-294-002
Titre	Vulnérabilité dans Samba
Date de la première version	13 juillet 2006
Date de la dernière version	02 août 2006
Source(s)	Bulletin de sécurité Samba du 10 juillet 2006
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 à distance.

## 2 Systèmes affectés

Les versions de Samba 3.0.1 à 3.0.22.

## 3 Description

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

Une vulnérabilité a été identifiée dans le démon `smbd` de Samba. Il maintient des structures de données en interne pour suivre les connexions actives de partages. Sous certaines conditions, une personne malveillante peut profiter de cette vulnérabilité pour augmenter l'espace mémoire alloué à Samba et provoquer un arrêt du service.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Bulletin de sécurité du projet Samba du 10 juillet 2006 :  
<http://www.samba.org/samba/security/CAN-2006-3403.html>
- Bulletin de sécurité SGI 20060703-01-P du 31 juillet 2006 :  
<ftp://patches.sgi.com/support/free/security/advisories/20060703-01-U.asc>
- Bulletin de sécurité Gentoo GLSA-200607-10 du 25 juillet 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200607-10.xml>
- Bulletin de sécurité Suse SUSE-SR:2006:017 du 21 juillet 2006 :  
<http://lists.suse.com/archive/suse-security-announce/2006-jul/0007.html>
- Bulletin de sécurité Debian DSA-1110 du 16 juillet 2006 :  
<http://www.us.debian.org/security/2006/dsa-1110/>
- Bulletin de sécurité RedHat RHSA-2006:0591 du 25 juillet 2006 :  
<http://rhn.redhat.com/errata/RHSA-2006-0591.html>
- Référence CVE CVE-2006-3403 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3403>
- Bulletin de sécurité d'Ubuntu USN-314-1 du 12 juillet 2006 :  
<http://www.ubuntu.com/usn/usn-314-1>
- Bulletin de sécurité Mandriva MDKSA-2006:120 du 10 juillet 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:120>
- Bulletin de sécurité FreeBSD du 10 juillet 2006 :  
<http://www.vuxml.org/freebsd/>

### Gestion détaillée du document

**13 juillet 2006** version initiale ;

**21 juillet 2006** ajout du bulletin de sécurité FreeBSD.

**02 août 2006** ajout des références aux bulletins de sécurité Gentoo, RedHat, Suse, Debian et SGI.