

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-2010-AVI-429>

---

### Gestion du document

Référence	CERTA-2010-AVI-429-001
Titre	Vulnérabilité dans Samba
Date de la première version	14 septembre 2010
Date de la dernière version	21 septembre 2010
Source(s)	Annonce de la version Samba 3.5.5
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

Samba 3.5.4 et versions précédentes.

## 3 Résumé

Un débordement de mémoire est présent dans le serveur Samba et peut être exploité par un utilisateur malveillant pour exécuter du code arbitraire à distance.

## 4 Description

Le serveur Samba ne vérifie pas correctement les identifiants Windows (SID). Ce défaut peut être utilisé pour provoquer un débordement de mémoire par un utilisateur malveillant et exécuter du code arbitraire à distance.

## 5 Solution

La version 3.5.5 de Samba corrige ce problème.

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

## 6 Documentation

- Annonce de la version Samba 3.5.5 du 14 septembre 2010 :  
<http://us1.samba.org/samba/history/samba-3.5.5.html>
- Bulletin de sécurité Samba CVE-2010-2069 du 14 septembre 2010 :  
<http://us1.samba.org/samba/security/CVE-2010-2069.html>
- Bulletin de sécurité Debian DSA-2109 du 16 septembre 2010 :  
<http://www.debian.org/security/2010/dsa-2109>
- Référence CVE CVE-2010-3069 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3069>

## Gestion détaillée du document

**14 septembre 2010** version initiale.

**21 septembre 2010** ajout de la référence au bulletin Debian.