



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 mai 2007  
N° CERTA-2007-AVI-219-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-2007-AVI-219>

---

### Gestion du document

Référence	CERTA-2007-AVI-219-001
Titre	Multiples vulnérabilités dans Samba
Date de la première version	15 mai 2007
Date de la dernière version	16 mai 2007
Source(s)	Bulletins de sécurité Samba du 14 mai 2007
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

- Samba 3.x versions antérieures à 3.0.25.

## 3 Résumé

De multiples vulnérabilités présentes dans Samba permettent à un utilisateur distant d'exécuter du code arbitraire et d'élever ses privilèges.

## 4 Description

Trois vulnérabilités sont présentes dans la version 3 de Samba :

- la première (CVE-2007-2444), présente dans la fonction de traduction des noms d'utilisateurs du service smbld, permet à un utilisateur connecté et authentifié au service d'élever ses privilèges ;

- la seconde (*CVE-2007-2446*), permet à un utilisateur malveillant connecté et authentifié au service d'exécuter du code arbitraire par le biais d'une requête MS-RPC spécialement conçue ;
- la dernière (*CVE-2007-2447*), dans le cas où l'option *username map script* est présente dans le fichier de configuration `smb.conf` de Samba, permet à un utilisateur malveillant connecté et authentifié au service d'exécuter du code arbitraire par le biais d'une requête MS-RPC spécialement conçue lors de la mise à jour du mot de passe d'un utilisateur.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Samba CVE-2007-2444 du 14 mai 2007 :  
<http://samba.org/samba/security/CVE-2007-2444.html>
- Bulletin de sécurité Samba CVE-2007-2446 du 14 mai 2007 :  
<http://samba.org/samba/security/CVE-2007-2446.html>
- Bulletin de sécurité Samba CVE-2007-2447 du 14 mai 2007 :  
<http://samba.org/samba/security/CVE-2007-2447.html>
- Bulletin de sécurité Mandriva MDKSA-2007:104 du 14 mai 2007 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:104>
- Bulletin de sécurité RedHat RHSA-2007:0354 du 14 mai 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0354.html>
- Référence CVE CVE-2007-2444 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2444>
- Référence CVE CVE-2007-2446 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2446>
- Référence CVE CVE-2007-2447 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447>
- Bulletin de sécurité Debian DSA-1291 du 15 mai 2007 :  
<http://www.debian.org/security/2007/dsa-1291>
- Bulletin de sécurité Ubuntu USN-460 du 16 mai 2007 :  
<http://www.ubuntu.com/usn/usn-460-1>
- Bulletin de sécurité Gentoo GLSA 200705-15 du 15 mai 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200705-15.xml>

## Gestion détaillée du document

**15 mai 2007** version initiale.

**16 mai 2007** ajout des références aux bulletins de sécurité Debian, Ubuntu et Gentoo.