

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans OpenLDAP

---

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-383>

---

### Gestion du document

Référence	CERTA-2006-AVI-383
Titre	Vulnérabilités dans OpenLDAP
Date de la première version	06 septembre 2006
Date de la dernière version	-
Source(s)	Bulletin de mise à jour du projet OpenLDAP
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

OpenLDAP 2.3.25 ainsi que les versions antérieures.

## 3 Description

Des vulnérabilités ont été identifiées dans l'application OpenLDAP qui met en œuvre le protocole LDAP (Lightweight Directory Access Protocol). Ce protocole sert à gérer des annuaires de bases d'informations sur le réseau, comme par exemple des coordonnées de personnes.

Suivant ce protocole, le DN (pour Distinguished Name) représente le nom d'une entrée sous la forme du chemin d'accès à celle-ci, depuis le sommet d'un arbre relationnel (un peu comme un chemin ou path sous Unix).

L'une des vulnérabilités permettrait à un utilisateur malveillant, ayant un accès `selfwrite` sur un attribut, de lui ajouter ou de supprimer non pas son DN, mais un DN quelconque.

## **4 Solution**

Se référer à la mise à jour du projet OpenLDAP pour l'obtention des correctifs (cf. section Documentation).

## **5 Documentation**

- Site du projet OpenLDAP :  
<http://www.openldap.org>
- Mise à jour 2.3.27 du 19 août 2006 du projet OpenLDAP :  
<http://http://www.openldap.org/software/download/>

## **Gestion détaillée du document**

**06 septembre 2006** version initiale.