

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2011-AVI-599>

---

### Gestion du document

Référence	CERTA-2011-AVI-599
Titre	Vulnérabilité dans OpenLDAP
Date de la première version	28 octobre 2011
Date de la dernière version	–
Source(s)	Référence CVE-2011-4079 de l'USCERT/NIST du 27 octobre 2011
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

*OpenLDAP* versions 2.4.26 et antérieures.

## 3 Résumé

Une vulnérabilité dans *OpenLDAP* permet de réaliser un déni de service à distance.

## 4 Description

Une vulnérabilité a été découverte dans *OpenLDAP*. Un utilisateur authentifié peut, en mettant une chaîne vide à un attribut particulier, provoquer un déni de service à distance.

## 5 Solution

Un correctif a été publié dans le `git` d'*OpenLDAP*.

## 6 Documentation

- Référence CVE-2011-4079 de l'USCERT/NIST du 27 octobre 2011  
<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4079>
- Adresse du `git` d'*OpenLDAP* :  
<http://www.openldap.org/software/repo/openldap.git/>
- Référence CVE CVE-2011-4079 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4079>

## Gestion détaillée du document

**28 octobre 2011** version initiale.