



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 octobre 2007
N° CERTA-2007-AVI-460

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-2007-AVI-460>

Gestion du document

Référence	CERTA-2007-AVI-460
Titre	Vulnérabilités dans OpenLDAP
Date de la première version	29 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de révision 2.3.39 d'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

Déni de service à distance.

2 Systèmes affectés

OpenLDAP, versions antérieures à la version 2.3.39.

3 Résumé

Plusieurs vulnérabilités permettent à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Plusieurs vulnérabilités affectent OpenLDAP :

- la fonction `add_filter_attrs()` ne gère pas correctement la fin de certaines chaînes de caractères. Ce défaut permet à un utilisateur malveillant de provoquer un déni de service à distance par épuisement de la mémoire ;

- les données entrées par l'utilisateur pour l'attribut `objectClasses` ne sont pas normalisées de manière assez stricte. Ceci permet à un utilisateur malveillant de provoquer un arrêt inopiné du serveur, à distance.

5 Solution

La version 2.3.39 corrige ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site du projet OpenLDAP :
<http://www.openldap.org/software/release/changes.html>
- Site de téléchargement du projet OpenLDAP :
<http://www.openldap.org/software/download/>
- Référence CVE CVE-2007-5707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5707>
- Référence CVE CVE-2007-5708 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5708>

Gestion détaillée du document

29 octobre 2007 version initiale.