

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-2008-AVI-081>

Gestion du document

Référence	CERTA-2008-AVI-081-001
Titre	Vulnérabilité dans OpenLDAP
Date de la première version	13 février 2008
Date de la dernière version	10 avril 2008
Source(s)	
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

OpenLDAP, versions 2.3.x.

3 Résumé

Une vulnérabilité dans *OpenLDAP* permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

La fonction *modrdn* sert à modifier les noms relatifs (RDN ou *Relative Distinguished Name*). Une erreur dans cette fonction est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance sur un serveur vulnérable.

5 Solution

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

6 Documentation

- Site de téléchargement du projet OpenLDAP :
<http://www.openldap.org/its/index.cgi/Software%20Bugs?id=5358>
- Bulletin de sécurité Debian DSA 1541-1 du 08 avril 2008 :
<http://lists.debian.org/debian-security-announce/2008/msg00111.html>
- Bulletin de sécurité Gentoo GLSA-200803-28 du 19 mars 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200803-28.xml>
- Bulletin de sécurité Mandriva MDKSA-2008:058 du 05 mars 2008 :
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité RedHat RHSA-2008:0110-3 du 21 février 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0110-3.html>
- Bulletin de sécurité Ubuntu USN-584-1 du 05 mars 2008 :
<http://www.ubuntulinux.org/usn/usn-584-1>
- Référence CVE CVE-2007-5708 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5708>
- Référence CVE CVE-2007-5707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5707>
- Référence CVE CVE-2007-6698 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6698>
- Référence CVE CVE-2008-0658 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0658>

Gestion détaillée du document

13 février 2008 version initiale.

13 février 2008 ajout des références Debian, Gentoo, Mandriva, Redhat, Ubuntu.