Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2010
N° CERTA-2010-AVI-325-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans OpenLDAP

Gestion du document

Référence	CERTA-2010-AVI-325-002
Titre	Multiples vulnérabilités dans OpenLDAP
Date de la première version	20 juillet 2010
Date de la dernière version	10 août 2010
Source(s)	Rapport d'erreurs OpenLDAP n6570 du 06 juillet 2010
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 ;
- déni de service à distance.

2 Systèmes affectés

OpenLDAP versions 2.4.22 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans `OpenLDAP` permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités relatives à la gestion des requêtes de type *modrdn* sont présentes dans `OpenLDAP`. Elles permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire par le biais de requêtes construites de façon particulière.

5 Solution

La version 2.4.23 corrige le problème :
http://www.openldap.org/software/download

6 Documentation

- Rapport d'erreurs OpenLDAP n6570 du 06 juillet 2010 :
  http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6570
- Liste des changements apportés à la version 2.4.23 de OpenLDAP :
  http://www.openldap.org/software/release/changes.html
- Bulletin de sécurité RedHat RHSA-2010-0542 du 20 juillet 2010 :
  https://rhn.redhat.com/errata/RHSA-2010-0542.html
- Bulletin de sécurité RedHat RHSA-2010-0543 du 20 juillet 2010 :
  https://rhn.redhat.com/errata/RHSA-2010-0543.html
- Bulletin de sécurité Ubuntu USN-965-1 du 09 août 2010 :
  http://www.ubuntu.com/usn/usn-965-1
- Bulletin de sécurité SuSE SUSE-SR:2010:014 du 02 août 2010 :
  http://lists.opensuse.org/opensuse-security-announce/2010-08/msg00001.html
- Bulletin de sécurité Debian DSA-2077 du 29 juillet 2010 :
  http://lists.debian.org/debian-security-announce/2010/msg00122.html
- Référence CVE CVE-2010-0211 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0211
- Référence CVE CVE-2010-0212 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0212

Gestion détaillée du document

20 juillet 2010 version initiale ;
21 juillet 2010 ajout des bulletins de sécurité RedHat du 20 juillet 2010.
10 août 2010 ajout des références aux bulletins de sécurité SuSE, Ubuntu et Debian.