

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Novell eDirectory

---

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-159>

---

### Gestion du document

Référence	CERTA-2008-AVI-159
Titre	Vulnérabilité de Novell eDirectory
Date de la première version	25 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Novell du 24 mars 2008
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

- Novell eDirectory versions 8.8.1 et antérieures pour Solaris ;
- Novell eDirectory versions 8.8.1 et antérieures pour Windows 2000 ;
- Novell eDirectory versions 8.8.1 et antérieures pour Windows 2003 ;
- Novell eDirectory versions 8.8.1 et antérieures pour GNU/Linux ;
- Novell eDirectory versions 8.7.3.9 et antérieures pour Solaris ;
- Novell eDirectory versions 8.7.3.9 et antérieures pour Windows 2000 ;
- Novell eDirectory versions 8.7.3.9 et antérieures pour Windows 2003 ;
- Novell eDirectory versions 8.7.3.9 et antérieures pour GNU/Linux.

## 3 Résumé

Une vulnérabilité dans Novell eDirectory permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Une erreur est présente dans la mise en œuvre du protocole LDAP par Novell eDirectory. Cette faille permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire par le biais d'une requête LDAP construite de façon particulière.

## 5 Solution

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

## 6 Documentation

- Site de Novell :  
<http://www.novell.com>
- Bulletin de sécurité Novell du 24 mars 2008 :  
[http://secure-support.novell.com/KanisaPlatform/Publishing/411/3382120\\_f.SAL\\_Public.html](http://secure-support.novell.com/KanisaPlatform/Publishing/411/3382120_f.SAL_Public.html)
- Référence CVE CVE-2008-0924 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0924>

## Gestion détaillée du document

25 mars 2008 version initiale.