



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 mai 2008  
N° CERTA-2008-AVI-248

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Red Hat Directory Server

---

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-248>

---

### Gestion du document

Référence	CERTA-2008-AVI-248
Titre	Vulnérabilité dans Red Hat Directory Server
Date de la première version	19 mai 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Red Hat 0268 et 0269 du 9 mai 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

*Red Hat Directory Server 7.1, 8 EL4, 8 EL5 et versions antérieures.*

## 3 Résumé

*Red Hat Directory Server* est un serveur d'annuaire reposant sur LDAP. Il permet de gérer, entre autres, les identités des utilisateurs, leurs droits d'accès et leurs options de connexions. Une vulnérabilité liée au traitement des requêtes LDAP a été corrigée.

## 4 Description

Une vulnérabilité affecte le traitement des requêtes au format LDAP à l'aide d'expressions régulières. Une personne mal intentionnée peut provoquer un dépassement de mémoire à l'aide d'une requête spécifiquement créée.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité RedHat RHSA-2008:0268 du 09 mai 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0268.html>
- Bulletin de sécurité RedHat RHSA-2008:0269 du 09 mai 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0269.html>
- Référence CVE CVE-2008-1677 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1677>

## Gestion détaillée du document

**19 mai 2008** version initiale.