

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans RedHat 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-2011-AVI-102>

---

### Gestion du document

Référence	CERTA-2011-AVI-102
Titre	Vulnérabilités dans RedHat Directory Server
Date de la première version	23 février 2011
Date de la dernière version	–
Source	Bulletin de sécurité RedHat RHSA-2011:0293 du 22 février 2011
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

RedHat Directory Server v8 EL4 et EL5.

## 3 Résumé

Plusieurs vulnérabilités dans l'annuaire RedHat Directory Server permettent à un utilisateur malveillant de provoquer un déni de service à distance ou d'élever ses privilèges.

## 4 Description

Trois vulnérabilités de RedHat Directory Server viennent d'être corrigées :

- le lancement simultané de recherches d'un certain type par un utilisateur distant non authentifié permet de provoquer un arrêt inopiné du serveur ;

- un défaut de positionnement des droits existe quand plusieurs serveurs annuaire s'exécutent sur la même machine, avec des comptes système non privilégiés. Ce défaut est exploitable par un utilisateur malveillant local pour provoquer un déni de service ;
- plusieurs scripts accompagnant le paquet RedHat Directory Server donnent à une variable d'environnement une valeur vide. Ceci peut être mis à profit par un utilisateur local pour élever ses privilèges.

## 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-2011:0293 du 22 février 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-0293.html>
- Référence CVE CVE-2011-0019 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0019>
- Référence CVE CVE-2011-0022 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0022>
- Référence CVE CVE-2011-0532 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0532>

## Gestion détaillée du document

23 février 2011 version initiale.