

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-432>

Gestion du document

Référence	CERTA-2008-AVI-432
Titre	Vulnérabilités dans Red Hat Directory Server
Date de la première version	29 août 2008
Date de la dernière version	–
Source(s)	Bulletin Red Hat RHSA-2008:0602-13 du 27 août 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

Déni de service à distance.

2 Systèmes affectés

Red Hat Directory Server 8.

3 Résumé

Deux vulnérabilités de Red Hat Directory Server permettent à un utilisateur malveillant de réaliser un déni de service à distance.

4 Description

Une première vulnérabilité réside dans un défaut de gestion de la mémoire. Son exploitation peut se traduire par une utilisation de toute la mémoire disponible et provoquer l'arrêt inopiné du serveur.

Une deuxième vulnérabilité concerne le traitement de certaines requêtes de recherche LDAP. Un utilisateur malveillant peut, en utilisant un motif particulier, provoquer l'utilisation sans limite de temps de la totalité du processeur.

5 Solution

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

6 Documentation

- Bulletin de sécurité Red Hat RHSA-2008:0602-13 du 27 août 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0602.html>
- Référence CVE CVE-2008-2930 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2930>
- Référence CVE CVE-2008-3283 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3283>

Gestion détaillée du document

29 août 2008 version initiale.