

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Directory Server Enterprise Edition

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-2009-AVI-561>

Gestion du document

Référence	CERTA-2009-AVI-561
Titre	Multiples vulnérabilités dans Directory Server Enterprise Edition
Date de la première version	29 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun Solaris #270789 du 23 décembre 2009
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

- Sun Java System Directory Server Enterprise Edition version 6.0 ;
- Sun Java System Directory Server Enterprise Edition version 6.1 ;
- Sun Java System Directory Server Enterprise Edition version 6.2 ;
- Sun Java System Directory Server Enterprise Edition version 6.3 ;
- Sun Java System Directory Server Enterprise Edition version 6.3.1 sans le correctif 141958-01.

3 Résumé

De multiples vulnérabilités dans *Directory Server Enterprise Edition* permettent de réaliser un déni de service à distance ou de bénéficier des privilèges d'un autre utilisateur.

4 Description

De multiples vulnérabilités ont été découvertes dans *Directory Server Enterprise Edition* versions 6.x :

- sous certaines conditions, l'opération d'un client peut être exécutée avec les privilèges d'un autre client ;
- en envoyant des paquets spécifiquement constitués, il est possible d'empêcher le serveur de répondre aux nouvelles connexions ;
- en utilisant un client `psearch` spécifique, il est possible d'empêcher le serveur d'envoyer des réponses aux autres clients `psearch`.

5 Solution

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

6 Documentation

- Bulletin de sécurité Sun Solaris #270789 du 23 décembre 2009 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270789-1>

Gestion détaillée du document

29 décembre 2009 version initiale.