



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 août 2002
N° CERTA-2002-AVI-180

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur Oracle Net Listener

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-2002-AVI-180>

Gestion du document

Référence	CERTA-2002-AVI-180
Titre	Vulnérabilités sur Oracle Net Listener
Date de la première version	19 août 2002
Date de la dernière version	–
Source(s)	Avis de sécurité #40 d'Oracle
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.

2 Systèmes affectés

- Oracle9i (versions 9.2.x et versions 9.0.x);
- Oracle8i (versions 8.1.x);
- Oracle7 (version 7.3.4).

3 Résumé

Deux vulnérabilités présentes sur l'outil de configuration Listener Control Utility peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service.

4 Description

Le service réseau Oracle Net Listener (port 1521/tcp par défaut) est le composant principal d' Oracle Net, l'application qui permet d'accéder à distance à une base de données Oracle. L'outil Listener Control Utility (lsnrctl) permet d'administrer ce service à distance.

Les droits par défaut du fichier de configuration du démon Oracle Net Listener (listener.ora) permettent à un utilisateur mal intentionné de modifier ce fichier. Les modifications effectuées peuvent provoquer un déni de service de l'outil Listener Control Utility lorsque l'administrateur utilisera cet outil.

Une seconde vulnérabilité présente dans la gestion des paramètres en entrée, peut entraîner un déni de service du service Oracle Net Listener.

5 Contournement provisoire

Sécuriser l'accès au fichier de configuration du « listener » :

- mettre l'option `set ADMIN_RESTRICTION_listener_name=ON;`
- restreindre les droits d'accès au seul propriétaire du fichier.

6 Solution

Appliquer le correctif correspondant à votre plate-forme (voir avis de sécurité Oracle, section documentation).

7 Documentation

Avis de sécurité #40 d'Oracle :

<http://otn.oracle.com/deploy/security/pdf/2002alert40rev1.pdf>

Gestion détaillée du document

19 août 2002 version initiale.