



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 août 2002  
N° CERTA-2002-AVI-191

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité sur Oracle Net**

---

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-191>

---

### Gestion du document

Référence	CERTA-2002-AVI-191
Titre	Vulnérabilité sur Oracle Net
Date de la première version	23 août 2002
Date de la dernière version	–
Source(s)	Avis de sécurité #38 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 9.0.x et 9.2.

## 3 Résumé

Une vulnérabilité présente dans Oracle Net de Oracle9i permet à un utilisateur mal intentionné de réaliser un déni de service sur le service Oracle Net Listener.

## 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.

Un utilisateur mal intentionné peut, par le biais de requêtes malicieusement construites, réaliser un déni de service du service réseau Oracle Net Listener.

## 5 Contournement provisoire

En attendant d'appliquer le correctif, il peut-être nécessaire de filtrer les adresses IP des postes clients du gestionnaire de base de données. Pour cela, dans le fichier `$ORACLE_HOME/NETWORK/ADMIN/SQLNET.ORA` ajouter les lignes suivantes :

- `tcp.validnode_checking = YES`
  
- `tcp.invited_nodes = (liste d'adresses IP)`
  
- `tcp.excluded_nodes = (liste d'adresses IP)`

## 6 Solution

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

## 7 Documentation

Avis de sécurité #38 d'Oracle :

<http://technet.oracle.com/deploy/security/pdf/2002alert38rev1.pdf>

## Gestion détaillée du document

23 août 2002 version initiale.