Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juillet 2001
N° CERTA-2001-AVI-073

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'Oracle

Gestion du document

Référence	CERTA-2001-AVI-073
Titre	Vulnérabilité d'Oracle
Date de la première version	05 juillet 2001
Date de la dernière version	–
Source(s)	Avis du CERT/CC CA-2001-16
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

- Exécution de code arbitraire sur le serveur avec les privilèges du compte utilisé par le processus, permettant aussi la modification de la base de données Oracle.
- Dans le cas de Windows NT ou 2000, ces privilèges sont ceux de `LOCAL_SYSTEM`.

2 Systèmes affectés

Oracle 8i.

3 Résumé

Une vulnérabilité de *TNS listener* permet de compromettre à distance une base de données Oracle sans authentification préalable.

4 Description

TNS (*Transparent Network Substate*) Listener est un élément de l'interface réseau des base de données Oracle 8i.

Une vulnérabilité de *TNS Listener* permet à un utilisateur mal intentionné d'obtenir, par le biais d'un débordement de mémoire, les privilèges de l'administrateur de la base de données sans authentification préalable.

5 Solution

Installer la version d'Oracle 9i qui ne présente pas cette vulnérabilité.

Un numéro à été donné à cette vulnérabilité : 1489683 et Oracle met au point un correctif pour les versions 8.1.7, 8.1.6 et 8.0.6 qui sera disponible à l'adresse suivante :

http://metalink.oracle.com

6 Documentation

- L'avis de sécurité de Oracle :
  http://otn.oracle.com/deploy/security/pdf/nai_net8_bof.pdf
- Le bulletin de sécurité du CERT/CC :
  http://www.cert.org/advisories/CA-2001-16.html

Gestion détaillée du document

05 juillet 2001 version initiale.