

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Oracle Database 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-2003-AVI-023>

---

### Gestion du document

Référence	CERTA-2003-AVI-023-001
Titre	Multiples vulnérabilités dans Oracle Database Server
Date de la première version	17 février 2003
Date de la dernière version	20 février 2003
Source(s)	Avis de sécurité #48 d'Oracle Avis de sécurité #49 d'Oracle Avis de sécurité #50 d'Oracle Avis de sécurité #51 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

- Exécution de code arbitraire ;
- déni de service.

## 2 Systèmes affectés

Oracle9i Database Server Release 2 et versions antérieures.

## 3 Résumé

Quatre vulnérabilités de type débordement de mémoire sont présentes dans Oracle Database Server.

## 4 Description

Oracle Database Server est le système de gestion de base de données d'Oracle.

Quatre vulnérabilités de type débordement de mémoire sont présentes dans Oracle Database Server. Ces vulnérabilités sont mentionnées dans les bulletins de sécurité suivants publiés sur le site d'Oracle :

- Buffer Overflow in DIRECTORY parameter of Oracle9i Database server ;
- Buffer Overflow in TZ\_OFFSET function of Oracle9i Database server ;
- Buffer Overflow in TO\_TIMESTAMP\_TZ function of Oracle9i Database server ;
- Buffer Overflow in ORACLE.EXE binary of Oracle9i Database server.

L'exploitation de ces vulnérabilités permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le serveur hébergeant la base de données.

La dernière vulnérabilité est exploitable par un utilisateur ne possédant pas d'authentification sur le système vulnérable.

## 5 Solution

Se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation) pour obtenir les correctifs.

## 6 Documentation

- Bulletin de sécurité #48 "Buffer Overflow in DIRECTORY parameter of Oracle9i Database server" : <http://otn.oracle.com/deploy/security/pdf/2003alert48.pdf>
- Bulletin de sécurité #49 "Buffer Overflow in TZ\_OFFSET function of Oracle9i Database server" : <http://otn.oracle.com/deploy/security/pdf/2003alert49.pdf>
- Bulletin de sécurité #50 "Buffer Overflow in TO\_TIMESTAMP\_TZ function of Oracle9i Database server" : <http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf>
- Bulletin de sécurité #51 "Buffer Overflow in ORACLE.EXE binary of Oracle9i Database server" : <http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf>
- Bulletin de sécurité #NISR16022003e "ORACLE bfilename function buffer overflow vulnerability" de NGSSoftware : <http://www.nextgenss.com/advisories/ora-bfilebo.txt>
- Bulletin de sécurité #NISR16022003c "ORACLE TZ\_OFFSET remote system buffer overrun" de NGSSoftware : <http://www.nextgenss.com/advisories/ora-tzofstbo.txt>
- Bulletin de sécurité #NISR16022003b "ORACLE TO\_TIMESTAMP\_TZ remote system buffer overrun" de NGSSoftware : <http://www.nextgenss.com/advisories/ora-tmstmpbo.txt>
- Bulletin de sécurité #NISR16022003a "ORACLE unauthenticated remote system compromise" de NGSSoftware : <http://www.nextgenss.com/advisories/ora-unauthrm.txt>
- Avis de sécurité CA-2003-05 "Multiple vulnerabilities in Oracle servers" du CERT/CC : <http://www.cert.org/advisories/CA-2003-05.html>

## Gestion détaillée du document

**17 février 2003** version initiale.

**20 février 2003** ajout condition d'exploitation de la vulnérabilité décrite dans le bulletin de sécurité #51 d'Oracle.  
Ajout documentation additionnelle.