

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Oracle9i Application 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-2002-AVI-002>

---

### Gestion du document

Référence	CERTA-2002-AVI-002
Titre	Multiples vulnérabilités dans Oracle9i Application Server
Date de la première version	02 janvier 2002
Date de la dernière version	–
Source(s)	Avis de sécurité #25 et #26 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

- Elévation de privilèges;
- compromission de données;
- déni de service.

## 2 Systèmes affectés

- Oracle9i Application Server pour :
- MS Windows NT/2000 Server;
  - Sun SPARC Solaris 2.6;
  - HP-UX 11.0.

## 3 Résumé

De multiples vulnérabilités présentes dans Oracle9i Application Server et dans la passerelle ModPL/SQL permettent à un utilisateur mal intentionné de réaliser une élévation de privilèges, d'accéder à des données non autorisées ou de réaliser un déni de service.

## 4 Description

ModPL/SQL est un module Apache livré avec Oracle9i Application Server permettant à des utilisateurs distants d'appeler des procédures PL/SQL.

Deux vulnérabilités (se référer à l'avis de sécurité #25 d'Oracle) sont présentes dans ce module:

- la première vulnérabilité permet de sortir de l'environnement du serveur Apache et accéder ainsi à des documents non autorisés résidant sur ce serveur;
- la seconde vulnérabilité, de type débordement de mémoire, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du compte utilisé par le serveur Apache.

Une autre vulnérabilité présente dans Oracle9i Application Server (systèmes MS Windows NT/2000 Server uniquement) permet à un utilisateur mal intentionné de réaliser un déni de service au moyen d'une requête http soigneusement choisie.

## 5 Solution

Installer les correctifs de l'éditeur (se référer à la section documentation).

## 6 Documentation

- Alerte de sécurité #25 d'Oracle "Vulnerabilities in MODPLSQL":  
<http://otn.oracle.com/deploy/security/pdf/modplsqli.pdf>
- Alerte de sécurité #26 d'Oracle "Potential DoS Vulnerability in Oracle9i Application Server":  
<http://otn.oracle.com/deploy/security/pdf/9iAS-GPF.pdf>

## Gestion détaillée du document

02 janvier 2002 version initiale.