

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités sur Oracle 9iAS v1.0.2.x

---

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-028>

---

## Gestion du document

Référence	CERTA-2002-AVI-028
Titre	Multiples vulnérabilités sur Oracle 9iAS v1.0.2.x
Date de la première version	11 février 2002
Date de la dernière version	–
Source(s)	Avis de sécurité #28 et #29 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;
- contournement des mécanismes d'authentification;

## 2 Systèmes affectés

Oracle9iAS version 1.0.2.x

## 3 Résumé

De multiples vulnérabilités présentes dans Oracle9iAS permettent à un utilisateur mal intentionné de réaliser une élévation de privilèges, d'accéder à des données non autorisées, de réaliser un déni de service et de contourner les paramètres d'authentification.

## 4 Vulnérabilités dans le module mod\_plsql

### 4.1 Description

Le module `mod_plsql v3.0.9.8.2` est une passerelle PL/SQL utilisée pour interfacier des applications web avec le langage PL/SQL, ce module présente plusieurs vulnérabilités :

- Une vulnérabilité de type « débordement de mémoire » permet à un utilisateur mal intentionné d'utiliser Oracle9iAS pour récupérer les droits du compte système sur les plateformes Microsoft.
- En utilisant certaines requêtes HTTP, un utilisateur mal intentionné peut provoquer un déni de service du module `mod_plsql` ou accéder à des fichiers du compte système.
- En utilisant les pages web pour la configuration de la passerelle `mod_plsql`, un utilisateur mal intentionné peut contourner l'authentification en utilisant les mots de passe par défaut pour administrer les points d'accès aux bases de données.

### 4.2 Contournement provisoire

Pour supprimer ces vulnérabilités il est nécessaire de :

- changer le chemin d'accès et configurer le fichier `wdbsvr.app`.
- d'appliquer le correctif approprié à la plateforme (voir Bulletin de sécurité #28 d'Oracle).

## 5 Vulnérabilité dans les modules OracleJSP and SQLJSP

### 5.1 Description

Le module OracleJSP/SQLJSP permet de faire interagir une base de données Oracle avec des applications web.

Lors d'une requête JSP sur un serveur OracleJSP, la page envoyée par l'utilisateur est traduite, compilée et exécutée. Trois fichiers intermédiaires contenant des informations de la base de données sont alors créés. Un utilisateur mal intentionné peut déduire l'emplacement et le nom de ces fichiers et récupérer des informations sensibles du système Oracle.

### 5.2 Contournement provisoire

Pour contourner cette vulnérabilité, il est nécessaire de modifier le fichier `httpd.conf` du module OracleJSP.

## 6 Vulnérabilités dans le module XSQL 1.0.x

### 6.1 Description

Oracle XSQL est une application qui permet d'intégrer les données résultant de requêtes SQL dans un document XML. Les vulnérabilités dans le module `XSQL 1.0.x` permettent à un utilisateur mal intentionné :

- d'exécuter un code arbitraire par le biais d'une vulnérabilité dans la requête HTTP.
- d'accéder à des informations sensibles du système Oracle en utilisant les applications XSQL.
- d'accéder au système via un exemple installé par défaut lors de l'installation d'Oracle.

### 6.2 Contournement provisoire

Pour supprimer ces vulnérabilités, il est conseillé (comme pour toutes les applications) de supprimer les exemples installés lors de l'installation. Il est également conseillé de déplacer le fichier `XSQLConfig.xml` dans un répertoire protégé.

## 7 Vulnérabilité dans le module EXTPROC

### 7.1 Description

Le module « External Procedure » (EXTPROC) permet l'appel de fonctionnalités du système d'exploitation.

Une vulnérabilité présente dans ce module permet à un utilisateur mal intentionné d'exécuter des commandes avec des privilèges administrateur.

## 7.2 Contournement provisoire

Si le module `EXTPROC` n'est pas nécessaire, il est recommandé de supprimer ce module.

Si ce module est nécessaire il est alors recommandé de créer deux processus « `LISTENER` », l'un étant utilisé par la base de données Oracle et l'autre par le module `EXTPROC`. La configuration de ces deux processus est détaillée dans le bulletin de sécurité #29 d'Oracle (voir Documentation).

## 8 Documentation

Avis de sécurité #28 de Oracle

[http://technet.oracle.com/deploy/security/pdf/ias\\_modplsqli\\_alert.pdf](http://technet.oracle.com/deploy/security/pdf/ias_modplsqli_alert.pdf)

Avis de sécurité #29 de Oracle

[http://technet.oracle.com/deploy/security/pdf/plsxtproc\\_alert.pdf](http://technet.oracle.com/deploy/security/pdf/plsxtproc_alert.pdf)

## Gestion détaillée du document

11 février 2002 version initiale.