

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité d'Oracle 10g

---

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-2007-ALE-016>

---

### Gestion du document

Référence	CERTA-2007-ALE-016
Titre	Vulnérabilité d'Oracle 10g
Date de la première version	16 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense du 07 novembre 2007
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 à distance.

## 2 Systèmes affectés

Oracle version 10g R2.

## 3 Résumé

Une vulnérabilité d'Oracle 10g permet à une personne distante d'exécuter du code arbitraire.

## 4 Description

Une vulnérabilité a été découverte dans la version 10g R2 de la base de données Oracle. Cette vulnérabilité est due à un débordement de mémoire au niveau de la procédure `XDB_PITRIG_PKG.PITRIG_DROPMETADATA`, via une très grande taille des arguments `OWNER` et `NAME`.

L'exploitation de cette vulnérabilité conduit à l'exécution de code arbitraire à distance.

## **5 Contournement provisoire**

L'éditeur reconnaît la faille et un correctif est déjà construit. Ce correctif sera disponible dans les prochaines mises à jour (Critical Patch Update, ou CPU), qui devrait avoir lieu en Janvier 2008.

En attendant, le CERTA recommande de :

- n'autoriser l'accès à la base Oracle qu'à partir d'adresse IP de confiance;
- filtrer en amont la taille des arguments passés à la base de données.

## **6 Documentation**

- Référence CVE CVE-2007-4517 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4517>
- Bulletin de sécurité iDefense du 07 novembre 2007 :  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=622>

## **Gestion détaillée du document**

**16 novembre 2007** version initiale.