



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 octobre 2006
N° CERTA-2006-AVI-457

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur les produits Oracle

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-2006-AVI-457>

Gestion du document

Référence	CERTA-2006-AVI-457
Titre	Multiples vulnérabilités sur les produits Oracle
Date de la première version	20 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuoct2006
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 ;
- déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Oracle Application Express 1.x ;
- Oracle Application Express 2.x ;
- Oracle Application Server 10g ;
- Oracle Collaboration Suite 10.x ;
- Oracle Database 10g ;
- Oracle Database 8.x ;
- Oracle Developer Suite 10g ;
- Oracle E-Business Suite 11i ;
- Oracle PeopleSoft Enterprise Portal Solutions 8.x ;
- Oracle PeopleSoft Enterprise Tools 8.x ;

- Oracle9i Application Server ;
- Oracle9i Collaboration Suite ;
- Oracle9i Database Enterprise Edition ;
- Oracle9i Database Standard Edition ;
- Oracle9i Developer Suite.

3 Description

Plusieurs vulnérabilités ont été découvertes dans les produits Oracle :

- Certaines de ces vulnérabilités sont dues à une erreur sur la vérification des paramètres d'entrées de certaines fonctions SQL. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné via une attaque d'injection SQL dans le but de porter atteinte à l'intégrité ou à la confidentialité des données présentes sur le système.
- D'autres vulnérabilités de type « débordement de mémoire » peuvent être utilisées par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire sur le système.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Oracle cpuoct2006 du 17 octobre 2006 :
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html>

Gestion détaillée du document

20 octobre 2006 version initiale.