



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2009
N° CERTA-2009-AVI-013

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des 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-2009-AVI-013>

Gestion du document

Référence	CERTA-2009-AVI-013
Titre	Vulnérabilités des produits Oracle
Date de la première version	14 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle du 13 janvier 2009
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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Oracle Database 9i, 10g et 11g ;
- Client Oracle SQL*Plus ;
- Oracle Secure Backup version 10.x ;
- Oracle TimesTen In-Memory Database version 7.x ;
- Oracle Application Server 10g ;
- Oracle Collaboration Suite 10g ;
- Oracle E-business Suite 11i et 12 ;
- Oracle Enterprise Manager Grid Control 10g ;
- Peoplesoft Enterprise HRMS ;
- JD Edwards Tools ;
- Oracle WebLogic Server, versions 7.x à 10. x ;
- Oracle WebLogic Portal, versions 8.x à 10. x.

3 Résumé

Plusieurs vulnérabilités affectent les produits Oracle. Elles permettent à un utilisateur malveillant de porter atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données.

4 Description

- Huit vulnérabilités, exploitables à distance après authentification, affectent les bases de données (Oracle Database). Elles permettent de porter atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données ;
- deux vulnérabilités affectent les clients SQL*Plus et permettent de porter atteinte à la confidentialité des données ;
- neuf vulnérabilités, exploitables à distance sans authentification, concernent Oracle Secure Backup. Quatre d'entre elles ne permettent qu'un déni de service. Les autres portent en plus atteinte à l'intégrité et à la confidentialité des données ;
- une vulnérabilité affecte la base de données résidente en mémoire, Oracle TimesTen In-Memory Database. Elle permet de porter atteinte à l'intégrité, à la confidentialité et à la disponibilité des données ;
- quatre vulnérabilités, dont trois sont exploitables sans authentification, affectent Oracle Application Server. Elles permettent de porter atteinte à la confidentialité ou à l'intégrité des données. Trois d'entre elles sont exploitables à distance ;
- une vulnérabilité de Oracle Collaboration Suite permet, à distance, à un utilisateur authentifié de lire indûment des données ;
- quatre vulnérabilités, dont une est exploitable sans authentification, sont présentes dans Oracle E-business Suite. Elles permettent de porter atteinte à la confidentialité ou à l'intégrité des données. Trois d'entre elles sont exploitables à distance ;
- une vulnérabilité concerne Oracle Enterprise Manager Grid Control. Elle permet à un utilisateur authentifié d'accéder à distance à des données ;
- cinq vulnérabilités sont présentes dans PeopleSoft. Elles permettent à un utilisateur authentifié de porter atteinte, à distance, à l'intégrité, à la confidentialité ou à la disponibilité des données ;
- une vulnérabilité de JD Edwards Tools permet à un utilisateur authentifié de lire indûment des données, à distance ;
- quatre vulnérabilités, exploitables à distance et sans authentification, affectent Oracle WebLogic Server. Elles permettent de porter atteinte à la confidentialité ou à l'intégrité des données.
- une vulnérabilité, exploitable à distance et sans authentification, affecte Oracle WebLogic Portal. Elle permet de porter atteinte à la confidentialité et à l'intégrité des données.

5 Solution

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

6 Documentation

- Bulletin de sécurité Oracle du 13 janvier 2009 :
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>
- Référence CVE CVE-2008-2623 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2623>
- Référence CVE CVE-2008-3973 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3973>
- Référence CVE CVE-2008-3974 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3974>
- Référence CVE CVE-2008-3978 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3978>
- Référence CVE CVE-2008-3979 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3979>

- Référence CVE CVE-2008-3981 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3981>
- Référence CVE CVE-2008-3997 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3997>
- Référence CVE CVE-2008-3999 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3999>
- Référence CVE CVE-2008-4006 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4006>
- Référence CVE CVE-2008-4007 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4007>
- Référence CVE CVE-2008-4014 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4014>
- Référence CVE CVE-2008-4015 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4015>
- Référence CVE CVE-2008-4016 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4016>
- Référence CVE CVE-2008-4017 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4017>
- Référence CVE CVE-2008-5436 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5436>
- Référence CVE CVE-2008-5437 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5437>
- Référence CVE CVE-2008-5438 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5438>
- Référence CVE CVE-2008-5439 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5439>
- Référence CVE CVE-2008-5440 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5440>
- Référence CVE CVE-2008-5441 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5441>
- Référence CVE CVE-2008-5442 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5442>
- Référence CVE CVE-2008-5443 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5443>
- Référence CVE CVE-2008-5444 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5444>
- Référence CVE CVE-2008-5445 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5445>
- Référence CVE CVE-2008-5446 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5446>
- Référence CVE CVE-2008-5447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5447>
- Référence CVE CVE-2008-5448 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5448>
- Référence CVE CVE-2008-5449 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5449>
- Référence CVE CVE-2008-5450 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5450>
- Référence CVE CVE-2008-5451 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5451>
- Référence CVE CVE-2008-5452 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5452>

- Référence CVE CVE-2008-5454 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5454>
- Référence CVE CVE-2008-5455 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5455>
- Référence CVE CVE-2008-5456 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5456>
- Référence CVE CVE-2008-5457 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5457>
- Référence CVE CVE-2008-5458 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5458>
- Référence CVE CVE-2008-5459 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5459>
- Référence CVE CVE-2008-5460 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5460>
- Référence CVE CVE-2008-5461 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5461>
- Référence CVE CVE-2008-5462 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5462>
- Référence CVE CVE-2008-5463 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5463>

Gestion détaillée du document

14 janvier 2009 version initiale.