



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 juillet 2008  
N° CERTA-2008-AVI-367

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits Oracle et Weblogic

---

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-2008-AVI-367>

---

### Gestion du document

Référence	CERTA-2008-AVI-367
Titre	Multiples vulnérabilités dans les produits Oracle et Weblogic
Date de la première version	16 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin Oracle du 14 juillet 2008
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Oracle Database 11g, 10g et 9i ;
- Oracle TimesTen in-Memory Database ;
- Oracle Application Server 10g ;
- Oracle E-business Suite 12 et 11i ;
- Oracle Enterprise Manager Database Control 11 et 10g ;
- Oracle Enterprise Manager Grid Control 10g ;
  
- Oracle PeopleSoft Enterprise PeopleTools 8.x ;
- Oracle PeopleSoft Enterprise CRM 8.x et 9.x ;

- *Oracle Hyperion Bi Plus 9.x* ;
- *Oracle Hyperion Performance Suite 8.x* ;
- *Oracle Weblogic Server 6, 7,8,9 et 10.x.*

### 3 Résumé

De nombreuses vulnérabilités affectent les produits *Oracle*. L'exploitation de certaines d'entre elles permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

### 4 Description

Onze vulnérabilités affectent les bases de données *Oracle Database*. Deux sont exploitables localement. L'exploitation à distance des neuf autres demande une authentification préalable. Un utilisateur malveillant exploitant ces vulnérabilités peut exécuter du code arbitraire à distance ou accéder indûment aux données.

Trois vulnérabilités concernent *Oracle TimesTen in-Memory Database*. Leur exploitation permet à un utilisateur malveillant de provoquer un déni de service à distance, sans requérir d'authentification.

Neuf vulnérabilités affectent *Oracle Application Server*. Elle permettent à un utilisateur malveillant non authentifié de provoquer un déni de service à distance, de modifier ou de lire des données de manière illégitime.

Six vulnérabilités de *E-business Suite* permettent de porter atteinte à la confidentialité ou à l'intégrité des données.

Deux vulnérabilités affectent *Oracle Enterprise Manager*. Leur exploitation permet à un utilisateur malveillant de porter atteinte à l'intégrité des données, à distance.

Sept vulnérabilités dans les produits *Oracle PeopleSoft* permettent à un utilisateur malveillant disposant d'une session valide de provoquer un déni de service à distance, de modifier ou de lire indûment des données.

Sept vulnérabilités sont présentes dans les serveurs *Oracle WebLogic*, dont quatre sont exploitables à distance sans authentification, une avec authentification et deux localement. Elles permettent à un utilisateur malveillant de provoquer un déni de service à distance, de modifier ou de lire 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 mise à jour Oracle du 14 juillet 2008 :  
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>
- Référence CVE CVE-2007-1359 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1359>
- Référence CVE CVE-2008-2576 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2576>
- Référence CVE CVE-2008-2577 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2577>
- Référence CVE CVE-2008-2578 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2578>
- Référence CVE CVE-2008-2579 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2579>
- Référence CVE CVE-2008-2580 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2580>
- Référence CVE CVE-2008-2581 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2581>
- Référence CVE CVE-2008-2582 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2582>



- Référence CVE CVE-2008-2609 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2609>
- Référence CVE CVE-2008-2610 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2610>
- Référence CVE CVE-2008-2611 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2611>
- Référence CVE CVE-2008-2612 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2612>
- Référence CVE CVE-2008-2613 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2613>
- Référence CVE CVE-2008-2614 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2614>
- Référence CVE CVE-2008-2615 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2615>
- Référence CVE CVE-2008-2616 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2616>
- Référence CVE CVE-2008-2617 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2617>
- Référence CVE CVE-2008-2618 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2618>
- Référence CVE CVE-2008-2620 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2620>
- Référence CVE CVE-2008-2621 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2621>
- Référence CVE CVE-2008-2622 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2622>

## **Gestion détaillée du document**

**16 juillet 2008** version initiale.