

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans la gestion des mots de passe sous Oracle Entreprise Manager Web site**

---

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-183>

---

### Gestion du document

Référence	CERTA-2002-AVI-183
Titre	Vulnérabilité dans la gestion des mots de passe sous Oracle Entreprise Manager Web site
Date de la première version	22 août 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle #39
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

Compromission de mots de passe.

## 2 Systèmes affectés

Oracle Entreprise Manager Web Site dans Oracle 9i Application Server 9.0.2 sous Linux et Unix.

## 3 Résumé

Une vulnérabilité a été découverte dans la gestion des mots de passe sous Oracle Entreprise Manager Web Site d'Oracle 9iAS.

## 4 Description

Oracle Entreprise Manager Web Site est une interface Web d'administration à distance fourni dans Oracle 9iAS. Le module Web Cache d'Oracle permet de mettre en cache les requêtes les plus fréquentes sur la base de données.

Un utilisateur mal intentionné peut avoir accès en local au mot de passe d'administration du module Web Cache.

## 5 Contournement provisoire

Il est conseillé de forcer le chiffrement du mot de passe dans le fichier de configuration `targets.xml` :

- Editer le fichier `$ORACLE_HOME/sysman/emd/targets.xml`.
- Remplacer toutes les lignes de type :

```
<Property NAME="authpwd" VALUE="administrator" /> par <Property NAME="authpwd" VALUE="a  
Note : FALSE est en lettres majuscules.
```

- Redémarrer Oracle Enterprise Manager Web site ou exécuter `emctl reload` sur la ligne de commande.

```
Note : Le redémarrage change la ligne précédemment saisie dans targets.xml par <Property NAME="authpwd" VA
```

## 6 Documentation

Bulletin de sécurité Oracle #39 :

<http://otn.oracle.com/deploy/security/pdf/2002alert39rev1.pdf>

## Gestion détaillée du document

22 août 2002 version initiale.