Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 octobre 2001
N° CERTA-2001-AVI-134

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le SGBD Oracle

Gestion du document

Référence	CERTA-2001-AVI-134
Titre	Multiples vulnérabilités dans le SGBD Oracle
Date de la première version	31 octobre 2001
Date de la dernière version	–
Source(s)	Bulletins de sécurité Oracle 19 et 20
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 avec élévation de privilèges ;
- Création et/ou modification de fichiers.

2 Systèmes affectés

Serveurs de base de données Oracle 8.0x, 8.1.x, et 9.0.1 sur toutes les plate-formes Unix.

3 Résumé

Une vulnérabilité des exécutables `otrcrep` et `oracle` dans le serveur de base de données permet à un utilisateur mal intentionné d'exécuter du code arbitraire et d'écraser ou créer des fichiers.

4 Description

Un utilisateur mal intentionné peut, par le biais d'un débordement de mémoire de la commande `otrcrep`, exécuter du code arbitraire avec les privilèges de l'utilisateur `Oracle` et/ou du groupe `dba`.

Une autre vulnérabilité permet, en invoquant astucieusement la commande `oracle` sous Unix, de bénéficier des droits du groupe `dba` pour écraser des fichiers de journalisation ou créer de nouveaux fichiers dans le répertoire `ORACLE_HOME/rdbms/log`.

Par ailleurs, en faisant pointer la variable `ORACLE_HOME` sur un répertoire arbitraire, il est possible de créer ou de modifier d'autres fichiers sur la machine.

5 Contournement provisoire

- Pour `octcrep` :
  - désactiver les fonctions de trace dans les paramètres du fichier `init<SID>.ora` comme suit (où <SID>est un numéro) : `Oracle_trace_enable=FALSE`
  - Modifier les permissions des fichiers pour tous les exécutables `Oracle Trace` :

```
chmod -s  otrccol otrcref otrcfmt otrcrep
chmod 751 otrccol otrcref otrcfmt otrcrep
```

- Pour l'exécutable `oracle` :
  changer les permissions de l'exécutable `oracle` : `chmod o-x oracle`

6 Solution

Selon Oracle, le correctif ne sera distribué qu'avec la nouvelle version d'Oracle : Oracle 9i release 2.
Consultez votre distributeur pour plus d'informations sur la mise à jour.

7 Documentation

Bulletins de sécurité Oracle :

- http://otn.oracle.com/deploy/security/pdf/otrcrep.pdf
- http://otn.oracle.com/deploy/security/pdf/oracle_race.pdf

Gestion détaillée du document

31 octobre 2001 version initiale.