Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2004
N° CERTA-2004-AVI-030

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur Oracle9i Database

Gestion du document

Référence	CERTA-2004-AVI-030
Titre	Vulnérabilités sur Oracle9i Database
Date de la première version	10 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité NGSSoftware
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

Elévation de privilèges.

2 Systèmes affectés

- Oracle9i Database Enterprise Edition v9.2.0.3 ;
- Oracle9i Database Standard Edition v9.2.0.3.

3 Résumé

Plusieurs vulnérabilités découvertes dans Oracle9i Database permettent à un utilisateur local de réaliser une élévation de privilèges (les privilèges `System` pour Windows ou `Oracle` pour Unix).

4 Description

Une faille de type débordement de mémoire présente sur la variable `char_expr` dans les deux fonctions de conversion `NUMTOYMINTERVAL` et `NUMTODSINTERVAL` permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur système.

Deux autres débordements de mémoire sont présents sur les paramètres `TZD` (Time Zone Difference) de la fonction `FROM_TZ` et `TIME_ZONE`.

5 Solution

Mettre à jour `Oracle9i Database` avec la version `Oracle9i Database Release 2, version 9.2.0.3` ou la version `9.2.0.4` en appliquant le patch 3 (cf site Metlalink Oracle, section documentation).

6 Documentation

- Site Metalink d'Oracle :
  http://metalink.oracle.com
- NGSSoftware : Oracle NUMTOYMINTERVAL Remote System Overflow :
  http://www.nextgenss.com/advisories/ora_numtoyminterval.txt
- NGSSoftware : Oracle NUMTODSINTERVAL Remote System Overflow :
  http://www.nextgenss.com/advisories/ora_numtodsinterval.txt
- NGSSoftware : Oracle TIME_ZONE Remote System Overrun :
  http://www.nextgenss.com/advisories/ora_time_zone.txt
- NGSSoftware : Oracle FROM_TZ Remote System Overrun :
  http://www.nextgenss.com/advisories/ora_from_tz.txt

Gestion détaillée du document

10 février 2004 version initiale.