



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 février 2004
N° CERTA-2004-AVI-046

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Oracle9i Application et Database Server

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-2004-AVI-046>

Gestion du document

Référence	CERTA-2004-AVI-046
Titre	Vulnérabilité dans Oracle9i Application et Database Server
Date de la première version	23 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité 65 d'Oracle
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.

2 Systèmes affectés

- Oracle9i Application Server seconde édition, versions 9.0.3.0 et 9.0.3.1 ;
- Oracle9i Application Server seconde édition, version 9.0.2.1 et les versions antérieures ;
- Oracle9i Application Server première édition, version 1.0.2.2 ;
- Oracle9i Database Server seconde édition, version 9.2.0.2 ;
- Oracle9i Database Server première édition, version 9.0.1.4.

3 Résumé

Une vulnérabilité a été découverte sur Oracle9i Application Server et Oracle9i Database Server qui permet à un utilisateur mal intentionné de réaliser un déni de service sur ces deux systèmes.

4 Description

Une vulnérabilité a été découverte dans l'analyse des données SOAP (Simple Object Access Protocol) des applications Oracle : Oracle9i Application Server et Oracle9i Database Server.

Un utilisateur mal intentionné peut, en envoyant une requête SOAP malicieusement construite, réaliser un déni de service des applications Oracle. Le risque est plus important pour les versions Oracle9i Application Server seconde édition version 9.2.0.1 et antérieures car l'authentification SOAP est désactivée par défaut.

5 Solution

Appliquer la mise à jour correspondant à votre version (cf. section documentation).

6 Documentation

- Correctif Oracle :
http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=259556.1
- Avis de sécurité 65 d'Oracle :
<http://otn.oracle.com/deploy/security/pdf/2004alert65.pdf>

Gestion détaillée du document

23 février 2004 version initiale.