



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2005
N° CERTA-2005-AVI-289

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des produits Oracle

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-2005-AVI-289>

Gestion du document

Référence	CERTA-2005-AVI-289
Titre	Multiples vulnérabilités des produits Oracle
Date de la première version	28 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Red DataBase Security du 21 juillet 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire ;
- exécution de commande arbitraire ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- élévation de privilèges ;
- cross-site scripting.

2 Systèmes affectés

- Oracle Application Server 10g ;
- Oracle Developer Suite 10g ;
- Oracle9i Application Server ;
- Oracle9i Developer Suite.

3 Description

De nombreuses vulnérabilités découvertes dans les produits Oracle permettent à un utilisateur distant de réaliser de attaques de type *cross-site scripting*, d'élever ses privilèges, d'exécuter des commandes ou du code arbitraire et de porter atteinte à la confidentialité et à l'intégrité des données présentes sur le systèmes.

4 Contournement provisoire

L'éditeur n'a pas publié de mise à jour de sécurité.

- Filtrer les requêtes URL, au moyen d'un proxy ou d'un pare-feu ;
- autoriser l'accès aux systèmes vulnérables uniquement au personnes de confiance ;
- interdire aux utilisateurs qui ne sont pas de confiance d'*uploader* des fichiers sur les systèmes vulnérables.

5 Documentation

- Bulletins de sécurité Red DataBase Security du 21 juillet :
 - http://red-database-security.com/advisory/oracle_reports_various_css.html
 - http://red-database-security.com/advisory/oracle_reports_read_any_xml.html
 - http://red-database-security.com/advisory/oracle_reports_read_any_file.html
 - http://red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
 - http://red-database-security.com/advisory/oracle_reports_run_any_os_command.html
 - http://red-database-security.com/advisory/oracle_forms_run_any_os_command.html
- Référence CVE CAN-2005-2371 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2371>
- Référence CVE CAN-2005-2372 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2372>
- Référence CVE CAN-2005-2378 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2378>
- Référence CVE CAN-2005-2379 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2379>

Gestion détaillée du document

version initiale.