



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 septembre 2004
N° CERTA-2004-AVI-284-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Nombreuses vulnérabilités dans les 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-2004-AVI-284>

Gestion du document

Référence	CERTA-2004-AVI-284-001
Titre	Nombreuses vulnérabilités dans les produits Oracle
Date de la première version	01 septembre 2004
Date de la dernière version	03 septembre 2004
Source(s)	Alerte de sécurité #68 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Oracle Database 10g Release 1, version 10.1.0.2 ;
- Oracle9i Database Server Release 2, versions 9.2.0.4 et 9.2.0.5 ;
- Oracle9i Database Server Release 1, versions 9.0.1.4, 9.0.1.5 et 9.0.4 ;
- Oracle8i Database Server Release 3, version 8.1.7.4 ;
- Oracle Entreprise Manager Grid Control 10g, version 10.1.0.2 ;
- Oracle Entreprise Manager Database Control 10g, version 10.1.0.2 ;
- Oracle Application Server 10g (9.0.4), versions 9.0.4.0 et 9.0.4.1 ;
- Oracle9i Application Server Release 2, versions 9.0.2.3 et 9.0.3.1 ;
- Oracle9i Application Server Release 1, version 1.0.2.2.

ces vulnérabilités n'affectent pas les versions suivantes :

- Oracle Database 10g Release 1, version 10.1.0.3 ;
- Oracle Entreprise Manager Grid Control 10g, version 10.1.0.3 ;
- Oracle Application Server 10g (9.0.4), version 9.0.4.2.

3 Résumé

Plusieurs vulnérabilités sont présentes dans les produits Oracle Database Server, Entreprise Manager et Application Server permettant à un individu mal intentionné d'exécuter du code arbitraire à distance. Les solutions Collaboration Suite et E-Business Suite 11i intégrant ces produits sont également affectés par ces vulnérabilités.

4 Solution

Appliquer les correctifs suivant la version affectée :

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1

5 Documentation

- Alerte de sécurité #68 d'Oracle :
<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>
- Bulletin de sécurité de NGS Software :
<http://www.nextgenss.com/advisories/oracle-01.txt>
- Bulletin de sécurité d'Intégrigy :
<http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm>
- Bulletin de sécurité d'Application Security :
<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>
- Bulletin de sécurité de Pete Finnigan :
<http://www.petefinnigan.com/alerts.htm>
- Référence CVE CAN-2004-0637 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0637>
- Référence CVE CAN-2004-0638 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0638>

Gestion détaillée du document

01 septembre 2004 version initiale.

03 septembre 2004 ajout de détails et de documentations.