



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2009
N° CERTA-2009-AVI-279

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2009-AVI-279>

Gestion du document

Référence	CERTA-2009-AVI-279
Titre	Multiples vulnérabilités dans des produits Oracle
Date de la première version	15 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle de juillet 2009
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 ;
- déni de service à distance.

2 Systèmes affectés

- Oracle Database 11g, versions 11.1.0.6, 11.1.0.7 ;
- Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 ;
- Oracle Database 10g, version 10.1.0.5 ;
- Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV ;
- Oracle Application Server 10g Release 2 (10.1.2), version 10.1.2.3.0 ;
- Oracle Application Server 10g Release 3 (10.1.3), versions 10.1.3.3.0, 10.1.3.4.0 ;
- Oracle Identity Management 10g, versions 10.1.4.0.1, 10.1.4.2.0, 10.1.4.3.0 ;
- Oracle E-Business Suite Release 12, version 12.1 ;
- Oracle E-Business Suite Release 12, version 12.0.6 ;
- Oracle E-Business Suite Release 11i, version 11.5.10.2 ;
- Oracle Enterprise Manager Database Control 11, versions 11.1.0.6, 11.1.0.7 ;
- Oracle Enterprise Manager Grid Control 10g Release 4, version 10.2.0.4 ;

- PeopleSoft Enterprise PeopleTools version 8.49 ;
- PeopleSoft Enterprise HRMS versions 8.9 et 9.0 ;
- Siebel Highly Interactive Client versions 7.5.3, 7.7.2, 7.8, 8.0, 8.1 ;
- Oracle WebLogic Server 10.3, 10.0MP1 ;
- Oracle WebLogic Server 9.0 GA, 9.1 GA, 9.2 à 9.2 MP3 ;
- Oracle WebLogic Server 8.1 à 8.1 SP6 ;
- Oracle WebLogic Server 7.0 à 7.0 SP7 ;
- Oracle Complex Event Processing 10.3 et WebLogic Event Server 2.0 ;
- Oracle JRockit R27.6.3 et les versions précédentes (JDK/JRE 6, 5, 1.4.2).

3 Résumé

De multiples vulnérabilités ont été découvertes dans les produits Oracle. L'exploitation de ces vulnérabilités permet de réaliser diverses actions malveillantes, dont l'exécution de code arbitraire à distance.

4 Description

Un grand nombre de vulnérabilités a été découvert dans les produits Oracle. L'exploitation de ces vulnérabilités permet de réaliser diverses actions malveillantes, dont l'exécution de code arbitraire à distance pour certaines.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Oracle de Juillet 2009 :
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>
- Référence CVE CVE-2009-0217 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0217>
- Référence CVE CVE-2009-0217 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0217>
- Référence CVE CVE-2009-0987 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0987>
- Référence CVE CVE-2009-1015 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1015>
- Référence CVE CVE-2009-1019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1019>
- Référence CVE CVE-2009-1020 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1020>
- Référence CVE CVE-2009-1021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1021>
- Référence CVE CVE-2009-1094 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1094>
- Référence CVE CVE-2009-1094 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1094>
- Référence CVE CVE-2009-1523 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1523>
- Référence CVE CVE-2009-1523 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1523>
- Référence CVE CVE-2009-1963 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1963>

- Référence CVE CVE-2009-1966 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1966>
- Référence CVE CVE-2009-1966 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1966>
- Référence CVE CVE-2009-1967 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1967>
- Référence CVE CVE-2009-1967 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1967>
- Référence CVE CVE-2009-1968 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1968>
- Référence CVE CVE-2009-1969 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1969>
- Référence CVE CVE-2009-1970 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1970>
- Référence CVE CVE-2009-1973 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1973>
- Référence CVE CVE-2009-1974 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1974>
- Référence CVE CVE-2009-1975 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1975>
- Référence CVE CVE-2009-1976 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1976>
- Référence CVE CVE-2009-1977 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1977>
- Référence CVE CVE-2009-1978 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1978>
- Référence CVE CVE-2009-1980 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1980>
- Référence CVE CVE-2009-1981 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1981>
- Référence CVE CVE-2009-1982 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1982>
- Référence CVE CVE-2009-1983 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1983>
- Référence CVE CVE-2009-1984 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1984>
- Référence CVE CVE-2009-1986 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1986>
- Référence CVE CVE-2009-1987 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1987>
- Référence CVE CVE-2009-1988 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1988>
- Référence CVE CVE-2009-1989 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1989>

Gestion détaillée du document

15 juillet 2009 version initiale.