

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Oracle 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-2012-AVI-577>

Gestion du document

Référence	CERTA-2012-AVI-577
Titre	Multiples vulnérabilités dans Oracle Database Server
Date de la première version	17 octobre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuoct2012-1515893 du 16 Octobre 2012
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 à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Oracle Core RDBMS 10.2.0.3
- Oracle Core RDBMS 10.2.0.4
- Oracle Core RDBMS 10.2.0.5
- Oracle Core RDBMS 11.1.0.7
- Oracle Core RDBMS 11.2.0.2
- Oracle Core RDBMS 11.2.0.3

3 Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Database Server*. L'une d'entre elle permet à un attaquant de récupérer la clef de session et le sel d'un utilisateur. Cela donne des informations sur le hash et rend donc plus facile l'attaque par force brute pour déterminer le mot de passe.

4 Solution

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

5 Documentation

- Bulletin de sécurité Oracle cpuoct2012-1515893 du 16 octobre 2012 :
<http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html>
- Référence CVE CVE-2012-3137 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3137>
- Référence CVE CVE-2012-1751 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1751>
- Référence CVE CVE-2012-3132 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3132>
- Référence CVE CVE-2012-3151 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3151>
- Référence CVE CVE-2012-3146 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3146>

Gestion détaillée du document

17 octobre 2012 version initiale.