

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Oracle Database Server

Gestion du document

Référence	CERTFR-2016-AVI-348
Titre	Multiples vulnérabilités dans Oracle Database Server
Date de la première version	19 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuoct2016-2881722 du 18 octobre 2016 Bulletin de sécurité Oracle cpuoct2016verbose-2881722 du 18 octobre 2016 Bulletin de sécurité Oracle cpuoct2016verbose-2881725 du 18 octobre 2016
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(s)

- exécution de code arbitraire à distance
- déni de service à distance
- déni de service
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Oracle Database Server versions antérieures à 5.0.4.00.07
- Oracle Database Server version 11.2.0.4
- Oracle Database Server version 12.1.0.2
- Oracle Secure Backup versions antérieures à 10.4.0.4.0
- Oracle Secure Backup versions antérieures à 12.1.0.2.0
- Oracle Big Data Graph versions antérieures à Prior to 1.2

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Database Server*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un déni de service.

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 cpuoct2016-2881722 du 18 octobre 2016
<http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html>
- Bulletin de sécurité Oracle cpuoct2016verbose-2881722 du 18 octobre 2016
<http://www.oracle.com/technetwork/security-advisory/cpuoct2016verbose-2881725.html#DB>
- Bulletin de sécurité Oracle cpuoct2016verbose-2881725 du 18 octobre 2016
<http://www.oracle.com/technetwork/security-advisory/cpuoct2016verbose-2881725.html#OSB>
- Référence CVE CVE-2010-5312
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5312>
- Référence CVE CVE-2015-0286
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0286>
- Référence CVE CVE-2015-1351
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1351>
- Référence CVE CVE-2015-7501
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7501>
- Référence CVE CVE-2016-3562
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3562>
- Référence CVE CVE-2016-5497
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5497>
- Référence CVE CVE-2016-5498
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5498>
- Référence CVE CVE-2016-5499
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5499>
- Référence CVE CVE-2016-5505
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5505>
- Référence CVE CVE-2016-5516
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5516>
- Référence CVE CVE-2016-5555
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5555>
- Référence CVE CVE-2016-5572
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5572>

Gestion détaillée du document

19 octobre 2016 version initiale.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-348
