Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 avril 2013
N° CERTA-2013-AVI-247

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Oracle Fusion Middleware

Gestion du document

Référence	CERTA-2013-AVI-247
Titre	Multiples vulnérabilités dans Oracle Fusion Middleware
Date de la première version	17 avril 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle CPUApr2013 du 16 avril 2013
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
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 Systèmes affectés

- Oracle JRockit versions R27.7.4 et antérieures
- Oracle JRockit versions R28.2.6 et antérieures
- Oracle HTTP Server version 11.1.1.6.0
- Oracle HTTP Server version 11.1.1.5.0
- Oracle HTTP Server version 10.1.3.5
- Oracle Web Services Manager version 11.1.1.6.0
- Oracle GoldenGate Veridata version 3.0.0.11
- Oracle COREid Access version 10.1.4.3.0
- Oracle Containers pour J2EE version 10.1.3.5
- Oracle WebCenter Content version 10.1.3.5.1

- Oracle WebCenter Content version 11.1.1.6.0
- Oracle WebCenter Interaction version 6.5.1
- Oracle WebCenter Interaction version 10.3.3.0
- Oracle WebLogic Server version 10.0.2
- Oracle WebLogic Server version 10.3.5
- Oracle WebLogic Server version 10.3.6
- Oracle WebLogic Server version 12.1.1
- Oracle WebCenter Capture version 10.1.3.5.1
- Oracle WebCenter Sites version 7.6.2
- Oracle WebCenter Sites version 11.1.1.6.0
- Oracle WebCenter Sites version 11.1.1.6.1
- Oracle Outside In Technology version 8.3.7
- Oracle Outside In Technology version 8.4.0

3 Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Fusion Middleware*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.

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 CPUApr2013 du 16 avril 2013
  http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
- Référence CVE CVE-2007-1862
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1862
- Référence CVE CVE-2009-0023
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0023
- Référence CVE CVE-2009-1191
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1191
- Référence CVE CVE-2009-1890
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1890
- Référence CVE CVE-2009-1955
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1955
- Référence CVE CVE-2009-1956
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1956
- Référence CVE CVE-2009-2699
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2699
- Référence CVE CVE-2010-0408
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0408
- Référence CVE CVE-2010-2068
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2068
- Référence CVE CVE-2010-2791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2791
- Référence CVE CVE-2012-0841
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0841
- Référence CVE CVE-2012-2751
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2751

- Référence CVE CVE-2012-4303
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4303
- Référence CVE CVE-2013-1497
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1497
- Référence CVE CVE-2013-1503
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1503
- Référence CVE CVE-2013-1504
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1504
- Référence CVE CVE-2013-1509
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1509
- Référence CVE CVE-2013-1514
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1514
- Référence CVE CVE-2013-1516
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1516
- Référence CVE CVE-2013-1522
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1522
- Référence CVE CVE-2013-1529
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1529
- Référence CVE CVE-2013-1542
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1542
- Référence CVE CVE-2013-1545
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1545
- Référence CVE CVE-2013-1553
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1553
- Référence CVE CVE-2013-1559
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1559
- Référence CVE CVE-2013-1565
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1565
- Référence CVE CVE-2013-2380
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2380
- Référence CVE CVE-2013-2390
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2390
- Référence CVE CVE-2013-2393
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2393

Gestion détaillée du document

17 avril 2013 version initiale.