

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans Oracle Java

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-2013-ALE-001>

Gestion du document

Référence	CERTA-2013-ALE-001-002
Titre	Vulnérabilités dans Oracle Java
Date de la première version	10 janvier 2013
Date de la dernière version	15 janvier 2013
Source(s)	Bulletin de sécurité Oracle Java version 1.7 du 13 janvier 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Oracle Java version 7 (première vulnérabilité)
- Versions antérieures à Oracle Java version 7 mise à jour 11 (deuxième vulnérabilité)

3 Résumé

Deux vulnérabilités ont été découvertes dans *Oracle Java*. La première vulnérabilité concerne la méthode "find-Class" de la classe *MBeanInstantiator*. Cette vulnérabilité est présente dans *Oracle Java* version 7.

La deuxième vulnérabilité se trouve dans la nouvelle API *Reflection* de *Oracle Java*. Cette nouvelle API est disponible à partir de la branche 1.7 du produit. Cette vulnérabilité est donc présente dans les versions antérieures à *Oracle Java* version 7 mise à jour 11.

L'association des deux vulnérabilités permet à un attaquant d'exécuter du code arbitraire à distance au moyen d'une page Web spécialement conçue sur les postes possédant une version de *Oracle Java* antérieure à 1.7.11. Ces vulnérabilités sont activement exploitées et largement diffusées.

4 Solution

Installer la dernière version stable de Oracle Java :

- Oracle Java version 1.7.11

5 Documentation

- Bulletin de sécurité Oracle Java version 1.7 du 13 janvier 2013 :
<http://www.oracle.com/technetwork/java/javase/7u11-relnotes-1896856.html>
- Référence CVE-2013-0422 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422>
- Référence CVE-2012-3174 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3174>

Gestion détaillée du document

10 janvier 2013 version initiale.

14 janvier 2013 ajout du correctif éditeur

15 janvier 2013 mise à jour systèmes affectés