

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Oracle Sun 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-2010-AVI-185>

Gestion du document

Référence	CERTA-2010-AVI-185
Titre	Vulnérabilités dans Oracle Sun Java
Date de la première version	16 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle CVE-2010-0886 du 15 avril 2010
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

JDK et JRE 6 pour Windows, Solaris et Linux.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Oracle Sun Java, dont une dans Java Deployment Toolkit qui permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été corrigées dont une concernant Java Deployment Toolkit. Ce dernier comprend un contrôle *ActiveX* pour Internet Explorer et un greffon pour Firefox destinés à faciliter le déploiement d'applications Java. Il offre une fonction qui permet de donner un argument au gestionnaire des fichiers *JNLP* (*Java Networking Launching Protocol*). Dans une configuration standard, ce gestionnaire est le

programme Java Web Start. La faiblesse du filtrage offert par la fonction de lancement permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

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 CVE-2010-0886 du 15 avril 2010 :
<http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html>
- Notes de mise à jour Sun JAVA 1.6.0_20 du 15 avril 2010 :
<http://java.sun.com/javase/6/webnotes/6u20.html>
- Référence CVE CVE-2010-0886 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0886>
- Référence CVE CVE-2010-0887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0887>

Gestion détaillée du document

16 avril 2010 version initiale.