Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 juin 2005
N° CERTA-2005-AVI-209-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des versions Sun de Java 2 Standard Edition

Gestion du document

Référence	CERTA-2005-AVI-209-002
Titre	Vulnérabilités des versions Sun de Java 2 Standard Edition
Date de la première version	14 juin 2005
Date de la dernière version	23 juin 2005
Source(s)	Bulletins de sécurité 101748 et 101749 de Sun
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

- Contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Tout système Windows, Solaris ou Linux utilisant :
- Java 2 Standard Edition (J2SE) version 5.0 (1.5.0) dans une version précédent l'« Update 2 » ;
- J2SE 1.4.2 dans une version antérieure à la 1.4.2_08.

3 Résumé

Des vulnérabilités peuvent être exploitées par des appliquettes quelconques pour élever leurs privilèges ce qui permet, par exemple, d'exécuter du code ou d'accéder à des fichiers arbitraires.

4 Description

Les failles concernent, d'une part, le « Java Runtime Environment » (JRE) et peuvent donc être exploitées par des sites malicieux à travers tout navigateur utilisant l'environnement de Sun, et d'autre part, l'outil « Java Web Start » qui peut être invoqué par un navigateur ou l'interface graphique du bureau.

5 Contournement provisoire

Désactiver l'invocation automatique de « Java Web Start » dans les navigateurs et dans l'explorateur pour Microsoft Windows.

Supprimer l'exécution des appliquettes Java dans les navigateurs ou la restreindre à des appliquettes de confiance.

6 Solution

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

7 Documentation

- Site officiel Java de Sun :
  http://java.sun.com
- Bulletin de sécurité Sun ID 101748 du 13 juin 2005 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-101748-1
- Bulletin de sécurité Sun ID 101749 du 13 juin 2005 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-101749-1
- Bulletin de sécurité Blackdown Java-Linux Blackdown-SA-2005-02 du 14 juin 2005 :
  http://www.blackdown.org/java-linux/java2-status/security/Blackdown-SA-2005-02.txt
- Bulletin de sécurité Gentoo GLSA 200506-14 du 19 juin 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200506-14.xml
- Bulletin de sécurité SUSE SUSE-SA:2005:032 du 22 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_32_java2.html
- Référence CVE CAN-2005-1974 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1974

Gestion détaillée du document

14 juin 2005 version initiale.

20 juin 2005 ajout des références aux bulletins de sécurité de Blackdown Java-Linux et Gentoo.

23 juin 2005 ajout de la référence au bulletin de sécurité de SUSE et ajout de la référence CVE CAN-2005-1974.