Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2009
N° CERTA-2009-AVI-119

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Java

Gestion du document

Référence	CERTA-2009-AVI-119
Titre	Multiples vulnérabilités dans Java
Date de la première version	26 mars 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité 254569, 254570, 254571, 254608, 254609, 254610 et 254611 du 24 mars 200
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

- Déni de service à distance ;
- exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- JDK et JRE 6 avec une mise à jour antérieure à la version 13 ;
- JDK et JRE 5.0 avec une mise à jour antérieure à la version 18 ;
- SDK et JRE versions antérieures à 1.4.2_20 ;
- SDK et JRE versions antérieures à 1.3.1_25.

3 Résumé

De multiples vulnérabilités du composant et de l'applet `Java` permettent à un individu distant de contourner la politique de sécurité, d'exécuter du code arbitraire et de réaliser un déni de service.

4 Description

De multiples vulnérabilités existent dans le composant et l'applet `Java` :

- la première est présente dans l'implémentation de l'initialisation de connexions *LDAP* et permet à un individu distant de réaliser un déni de service ;
- la deuxième est présente dans le client *LDAP* du *JRE* et permet à un individu distant d'exécuter du code arbitraire présent sur un serveur *LDAP* spécialement paramétré ;
- la troisième concerne les composants `Java` utilisant l'application *unpack200*, elle permet à un individu distant, par le biais de plusieurs débordements, d'élever ses privilèges au moyen d'une application `Java` spécialement construite ;
- la quatrième est un débordement de mémoire lors de la manipulation d'images, elle permet à un individu distant d'élever ses privilèges par le biais d'un fichier image spécialement construit ;
- la cinquième concerne la gestion du stockage temporaire de certains fichiers (*font files*), elle permet à un individu distant de réaliser un déni de service en remplissant l'espace de stockage ;
- la sixième concerne le service *JAX-WS*, présent dans l'implémentation du serveur HTTP, elle permet à un individu distant de réaliser un déni de service ;
- la septième concerne la machine virtuelle du *JRE*, elle permet à un individu distant de contourner la politique de sécurité et d'exécuter du code arbitraire ;
- la dernière concerne le composant `Java`, de multiples vulnérabilités de ce composant permettent à un individu distant de contourner la politique de sécurité, d'exécuter du code arbitraire et de réaliser un déni de service.

5 Solution

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

6 Documentation

- Bulletin de sécurité Sun Solaris #254569 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254569-1
- Bulletin de sécurité Sun Solaris #254570 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254570-1
- Bulletin de sécurité Sun Solaris #254571 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254571-1
- Bulletin de sécurité Sun Solaris #254608 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254608-1
- Bulletin de sécurité Sun Solaris #254609 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254609-1
- Bulletin de sécurité Sun Solaris #254610 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254610-1
- Bulletin de sécurité Sun Solaris #254611 du 24 mars 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-254611-1

Gestion détaillée du document

26 mars 2009 version initiale.