Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2007
N° CERTA-2007-AVI-348-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la machine Java d'IBM

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-2007-AVI-348

Gestion du document

Référence	CERTA-2007-AVI-348-002
Titre	Multiples vulnérabilités dans la machine Java d'IBM
Date de la première version	07 août 2007
Date de la dernière version	16 novembre 2007
Source(s)	Avis Redhat RHSA-2007:0817-2 du 06 août 2007
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 ;
- déni de service ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Sun Java Enterprise System 5.x (JSSE) 1.x ;
- Sun Java JDK 1.5.x ;
- Sun Java JDK 1.6.x ;
- Sun Java JRE 1.3.x ;
- Sun Java JRE 1.4.x ;
- Sun Java JRE 1.5.x / 5.x ;
- Sun Java JRE 1.6.x / 6.x ;
- Sun Java SDK 1.3.x ;
- Sun Java SDK 1.4.x.

3 Résumé

Plusieurs vulnérabilités dans les paquetages `java-1.4.2-ibm` permettent à un utilisateur malveillant de contourner la politique de sécurité du système vulnérable.

4 Description

Une première vulnérabilité, liée à `Java Web Start`, permet à un utilisateur d'élever ses privilèges et d'accéder indûment à des fichiers en lecture et en modification (CVE-2007-2435).

Une seconde vulnérabilité permet à une application (ou à une *applet*) d'élever ses privilèges et d'exécuter un code arbitraire sur la machine virtuelle (CVE-2007-3004).

Une troisième vulnérabilité permet de bloquer la machine virtuelle, provoquant un déni de service (CVE-2007-3005).

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200705-23 du 31 mai 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200705-23.xml
- Bulletin de sécurité Gentoo GLSA-200706-08 du 26 juin 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200706-08.xml
- Bulletin de sécurité RedHat RHSA-2007:0817 du 06 août 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0817.html
- Bulletin de sécurité RedHat RHSA-2007:0818 du 06 août 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0818.html
- Bulletin de sécurité RedHat RHSA-2007:0829 du 07 août 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0829.html
- Bulletin de sécurité SuSE SUSE-SA:2007:045 du 18 juillet 2008 :
  http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00007.html
- Bulletin de sécurité Avaya ASA-2007-199 du 23 mai 2007 :
  http://support.avaya.com/elmodocs2/security/ASA-2007-199.htm
- Avis du CERTA CERTA-2007-AVI-238 du 01 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-238/index.html
- Référence CVE CVE-2007-2435 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2435
- Référence CVE CVE-2007-2788 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2788
- Référence CVE CVE-2007-2789 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2789
- Référence CVE CVE-2007-3004 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3004
- Référence CVE CVE-2007-3005 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3005
- Référence CVE CVE-2007-3503 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3503
- Référence CVE CVE-2007-3655 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3655
- Référence CVE CVE-2007-3922 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3922
- Bulletin de sécurité HP OpenView c01269450 du 14 novembre 2007 :
  http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=c01269450

Gestion détaillée du document

07 août 2007 version initiale.

08 août 2007 modification des systèmes affectés, ajout des références CVE et des bulletins de sécurité des éditeurs SuSE, Red Hat, Avaya et Gentoo.

16 novembre 2007 ajout de la référence au bulletin de sécurité HP OpenView.