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 janvier 2006
N° CERTA-2005-AVI-474-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la machine virtuelle Java de Sun

Gestion du document

Référence	CERTA-2005-AVI-474-003
Titre	Multiples vulnérabilités dans la machine virtuelle Java de Sun
Date de la première version	30 novembre 2005
Date de la dernière version	16 janvier 2006
Source(s)	Bulletin de sécurité Sun du 28 novembre 2005
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

- SDK et JRE versions 1.3.1 Update 15 (1.3.1_15) et antérieures ;
- SDK et JRE versions 1.4.2 Update 8 (1.4.2_08) et antérieures ;
- SDK et JRE versions 1.5.0 Update 3 (1.5.0_03) et antérieures.

3 Résumé

De multiples vulnérabilités dans la machine virtuelle Java de Sun permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

La machine virtuelle Java ou JRE (Java Runtime Environment) permet d'exécuter des applications Java. Plusieurs vulnérabilités présentes dans certaines API (Application Programming Interfaces)

Java permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une *applet* malicieusement construite.

5 Solution

- La version 1.3.1 Update 16 (1.3.1_16), ou version supérieure, du SDK ou de la JRE corrige le problème : http://java.sun.com/j2se/1.3/download.html
- La version 1.4.2 Update 9 (1.4.2_09), ou version supérieure, du SDK ou de la JRE corrige le problème : http://java.sun.com/j2se/1.4.2/download.html
- La version 1.5.0 Update 4 (1.5.0_04), ou version supérieure, du SDK ou de la JRE corrige le problème : http://java.sun.com/j2se/1.5.0/download.jsp

6 Documentation

- Site de l'éditeur : http://java.sun.com
- Bulletin de sécurité Sun #102050 du 28 novembre 2005 : http://sunsolve.sun.com/search/document.do?assetkey=1-26-102050-1
- Bulletin de sécurité Sun #102003 du 28 novembre 2005 : http://sunsolve.sun.com/search/document.do?assetkey=1-26-102003-1
- Bulletin de sécurité Sun #102017 du 28 novembre 2005 : http://sunsolve.sun.com/search/document.do?assetkey=1-26-102017-1
- Bulletin de sécurité Apple #302913 du 15 novembre 2005 : http://docs.info.apple.com/article.html?artnum=302913
- Bulletin de sécurité SUSE SUSE-SR:2006:001 du 13 janvier 2006 : http://www.novell.com/linux/security/advisories/2006_01_sr.html
- Bulletin de sécurité Gentoo GLSA 200601-10 du 16 janvier 2006 : http://www.gentoo.org/security/en/glsa/glsa-200601-10.xml
- Référence CVE CVE-2005-3904 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3904
- Référence CVE CVE-2005-3905 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3905
- Référence CVE CVE-2005-3906 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3906

Gestion détaillée du document

30 novembre 2005 version initiale.
02 décembre 2005 ajout de la référence au bulletin de sécurité Apple.
08 décembre 2005 corrections et précisions sur les versions impactées.
16 janvier 2006 ajout des références aux bulletins de sécurité SUSE et Gentoo et des références CVE.