Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 septembre 2005
N° CERTA-2005-AVI-344

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de la plateforme Java sous MacOS X

Gestion du document

Référence	CERTA-2005-AVI-344
Titre	Multiples vulnérabilités de la plateforme Java sous MacOS X
Date de la première version	14 septembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple du 13 septembre 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

- Elévation de privilèges ;
- divulgation d'information ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de Java 1.3.1 antérieures à 1.3.1_16 et 1.4.2 antérieures à 1.4.2_09 sont vulnérables.
Les mises à jour sont disponibles sur les systèmes Mac OS X Panther (Mac OS X 10.3) et MAC OS X Tiger (Mac OS X 10.4).

3 Description

Cinq vulnérabilités affectent la plate-forme Java sous Mac OS X.

- Une première vulnérabilité permet la corruption de fichiers ou la création arbitraire de fichiers (CAN-2005-2527) ;
- une deuxième vulnérabilité permet également la corruption de fichiers ou la création arbitraire de fichiers (CAN-2005-2528) ;

- une troisième vulnérabilité permet à un utilisateur local mal intentionné d'obtenir une élévation de privilèges (CAN-2005-2529) ;
- une quatrième vulnérabilité permet à une «appliquette» Java d'obtenir une élévation de privilèges (CAN-2005-2530) ;
- une cinquième vulnérabilité permet l'interception de trafic réseau à destination d'un *ServerSocket* particulier (CAN-2005-2538).

4 Solution

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

5 Documentation

- Site Internet d'apple :
  http://www.apple.com
- Bulletins de sécurité Apple :
  http://docs.info.apple.com/article.html?artnum=302265
  http://docs.info.apple.com/article.html?artnum=302266
- Référence CVE CAN-2005-2527 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2527
- Référence CVE CAN-2004-2528 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-2528
- Référence CVE CAN-2004-2529 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-2529
- Référence CVE CAN-2004-2530 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-2530
- Référence CVE CAN-2004-2538 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-2538

14 septembre 2005 version initiale.