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 juin 2004
N° CERTA-2004-AVI-154-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilités sur les systèmes IBM AIX 5.1 et 5.2



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-154-001 |
| Titre | Vulnérabilités sur les systèmes IBM AIX 5.1 et 5.2 |
| Date de la première version | 04 mai 2004 |
| Date de la dernière version | 14 juin 2004 |
| Source(s) | Avis de sécurité IBM |
| 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 ;
- perte de données ;
- exécution de code arbitraire.

## 2 Systèmes affectés

AIX versions 5.1 et 5.2.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans certaines commandes système et certaines commandes LVM (`Logical Volume Manager`) permettent à un utilisateur mal intentionné de réaliser un déni de service.

## 4 Description

Des dépassements de tampon présents dans les commandes système `putlvcb` et `getlvcb`, utilisées par les commandes LVM de plus haut niveau, permettent à un utilisateur local mal intentionné de réaliser un déni de service et dans certains cas d'exécuter du code arbitraire sur un système vulnérable.

D'autres vulnérabilités présentes dans certaines commandes des paquetages `bos.rte.console` et `bos.rte.serv_aid` permettent à un utilisateur local mal intentionné, via la création de liens symboliques, de réaliser une destruction de données.

# 5 Solution

Dans l'attente des correctifs disponibles prochainement (cf. avis de sécurité IBM), appliquer les correctifs d'urgence disponibles sur le site IBM.

- Correctif pour la vulnérabilité sur les commandes LVM :
  ftp://aix.software.ibm.com/aix/efixes/security/lvmcmd_efix.tar.Z
- Correctif pour la vulnérabilité sur les commandes systèmes :
  ftp://aix.software.ibm.com/aix/efixes/security/conscmd_efix.tar.Z

# 6 Documentation

- Avis de sécurité MSS-OAR-E01-2004:0544.2 :
  http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0544.2
- Avis de sécurité MSS-OAR-E01-2004:0543.2 :
  http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0543.2
- Référence CVE CAN-2004-0544 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0544
- Référence CVE CAN-2004-0545 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0545

# Gestion détaillée du document

**04 mai 2004** version initiale.
**14 juin 2004** ajout références CVE.