Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 décembre 2004
N° CERTA-2004-AVI-410

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Plusieurs vulnérabilités sur AIX



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-410 |
| Titre | Plusieurs vulnérabilités sur AIX |
| Date de la première version | 22 décembre 2004 |
| Date de la dernière version | – |
| Source(s) | Bulletins 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

- Elévation de privilèges ;
- exécution de code arbitraire.

## 2 Systèmes affectés

- AIX version 5.1.0 ;
- AIX version 5.2.0 ;
- AIX version 5.3.0.

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans les commandes `lsvpd`, `chcod` et le script `diag` sur le système AIX. Un utilisateur local mal intentionné peut exploiter ces vulnérabilités pour élever ses privilèges ou exécuter du code arbitraire sur le système.

# 4 Description

## 4.1 Vulnérabilité dans chcod

Une vulnérabilité est présente sur la commande `chcod`. Cette vulnérabilité permet à un utilisateur local mal intentionné qui fait partie du groupe `system` d'exécuter un code arbitraire sur le système avec les privilèges du super utilisateur.

## 4.2 Vulnérabilité dans lsvpd

Une vulnérabilité présente sur la commande `lsvpd` permet à un utilisateur mal inetntionné, via un binaire malicieusement construit placé dans une arborescence judicieusement choisie, d'élever ses privilèges sur le système.

## 4.3 Vulnérabilité dans le script `diag`

Une vulnérabilité est présente sur le script `diag`. Cette vulnérabilité permet à un utilisateur local non privilègié d'exécuter un code arbitraire avec les privilèges du super utilisateur sur le système vulnérable via l'utilisation des commandes appelées par ce script (`lscode, invscout, invscoutd, diag_exec`).

# 5 Solution

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

# 6 Documentation

- Bulletin de sécurité IBM MSS-0AR-E01-2004:2061.1 :
  http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.2061.1
- Bulletin de sécurité IBM MSS-0AR-E01-2004:2062.1 :
  http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.2062.1
- Bulletin de sécurité IBM MSS-0AR-E01-2004:2063.1 :
  http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.2063.1
- Bulletin de sécurité idefense du 20 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=170&type=vulnerabilities
- Bulletin de sécurité idefense du 20 décembre 2004 :
  http://www.idefense.com/application/poi/display?id=171&type=vulnerabilities
- Référence CVE CAN-2004-1054 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1054
- Référence CVE CAN-2004-1028 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1028

# Gestion détaillée du document

**22 décembre 2004** version initiale.