



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 février 2008  
N° CERTA-2008-AVI-102

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans IBM AIX

---

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-2008-AVI-102>

---

### Gestion du document

Référence	CERTA-2008-AVI-102
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	22 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM AIX du 21 février 2008
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 à distance.

## 2 Systèmes affectés

- IBM AIX 5.2 ;
- IBM AIX 5.3 ;
- IBM AIX 6.1.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans IBM AIX et permettent à un individu malveillant de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

Pegasus CIM Server for Directory d'IBM AIX est un outil de gestion d'objet fournissant des modèles communs d'information. Plusieurs vulnérabilités ont été découvertes dans ce produit et permettent via un dépassement de mémoire tampon de provoquer un déni de service à distance ou une exécution de code arbitraire.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité IBM du 21 février 2008 :  
<http://www14.software.ibm.com/webapp/set2/subscriptions/ijhifoeblist?mode=7&heading=AIX61&path=%2F200802%2F>
- Référence CVE CVE-2008-0003 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0003>
- Référence CVE CVE-2008-0495 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0495>

## Gestion détaillée du document

22 février 2008 version initiale.