



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 septembre 2007  
N° CERTA-2007-AVI-392

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2007-AVI-392>

---

### Gestion du document

Référence	CERTA-2007-AVI-392
Titre	Vulnérabilités dans IBM AIX
Date de la première version	06 septembre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité de IBM AIX
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 ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- IBM AIX 5.2 ;
- IBM AIX 5.3.

## 3 Résumé

De multiples vulnérabilités dans IBM AIX permettent à une personne malintentionnée d'effectuer un déni de service, d'élever ses privilèges et de porter atteinte à l'intégrité des données.

## 4 Description

De multiples vulnérabilités ont été identifiées dans IBM AIX :

- des débordements de mémoire présents dans certaines commandes ont des impacts inconnus ;
- une erreur inconnue au niveau de la commande `invscout` cause la suppression de certains fichiers ;
- une erreur de vérification de privilèges dans l’extension `perfstat` du noyau peut être exploitée pour changer des paramètres du noyau, ce qui peut causer l’arrêt inopiné du système.

## 5 Contournement Provisoire

Des correctifs temporaires ont été mis à disposition par IBM pour certaines des vulnérabilités (IY98506, IZ02717, IZ02718, IY98819, IY98804, IZ00997). Ces correctifs peuvent avoir certains effets de bord, il est recommandé de les tester avant un déploiement sur des systèmes en production.

## 6 Solution

Se référer aux bulletins de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

## 7 Documentation

- Liste des correctifs temporaires d’IBM pour AIX :  
<ftp://aix.software.ibm.com/aix/efixes/security/README>
- Emplacement des correctifs temporaires d’IBM pour AIX :  
<ftp://aix.software.ibm.com/aix/efixes/security>
- Bulletin de sécurité IBM IY94739 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY94739>
- Bulletin de sécurité IBM IY94761 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY94761>
- Bulletin de sécurité IBM IY97233 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY97233>
- Bulletin de sécurité IBM IY91132 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY91132>
- Bulletin de sécurité IBM IY91145 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY91145>
- Bulletin de sécurité IBM IY97309 du 03 août 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY97309>
- Bulletin de sécurité IBM IZ02717 du 31 août 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ02717>
- Bulletin de sécurité IBM IZ02718 du 31 août 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ02718>
- Bulletin de sécurité IBM IY98819 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY98819>
- Bulletin de sécurité IBM IY98804 du 06 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY98804>
- Bulletin de sécurité IBM IY97215 du 25 mai 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY97215>
- Bulletin de sécurité IBM IY95852 du 24 mai 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY95852>
- Bulletin de sécurité IBM IZ00997 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ00997>
- Bulletin de sécurité IBM IY98506 du 13 juin 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY98506>

# **Gestion détaillée du document**

**06 septembre 2007** version initiale.