

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-594>

---

### Gestion du document

Référence	CERTA-2008-AVI-594
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	11 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM AIX du 26 novembre 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

- Élévation de privilèges ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

IBM AIX 6.1.x.

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans IBM AIX et permettent à un utilisateur local malintentionné d'élever ses privilèges et de porter atteinte à l'intégrité des données.

## 4 Description

Plusieurs vulnérabilités permettant à un utilisateur local d'élever ses privilèges sont présentes dans le système d'exploitation IBM AIX :

- la première est relative à la commande `/usr/sbin/ndp` qui présente une erreur de type débordement de mémoire si le service `net.cd` est lancé ;

- la seconde concerne la commande `/usr/sbin/autoconf6` qui présente une erreur de type débordement de mémoire et peut être exploitée si la fonction RBAC est utilisée et que l'attaquant possède la permission :  
`aix.network.config.tcpip`;
- la troisième est relative à la commande `/usr/bin/enq` qui permet, sous certaines conditions, de supprimer des fichiers du système;
- la dernière concerne la commande `/usr/bin/crontab` qui permet, sous certaines conditions, de donner des privilèges élevés à l'éditeur qu'il appelle.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité AIX du 26 novembre 2008 :  
[http://aix.software.ibm.com/aix/efixes/security/aix61\\_advisory.asc](http://aix.software.ibm.com/aix/efixes/security/aix61_advisory.asc)
- Référence CVE CVE-2008-5384 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5384>
- Référence CVE CVE-2008-5385 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5385>
- Référence CVE CVE-2008-5386 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5386>
- Référence CVE CVE-2008-5387 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5387>

## Gestion détaillée du document

11 décembre 2008 version initiale.