

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-570>

Gestion du document

Référence	CERTA-2008-AVI-570
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	01 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.

2 Systèmes affectés

IBM AIX 6.1.x.

3 Résumé

Plusieurs vulnérabilités dans IBM AIX permettent à une personne malintentionnée d'élever ses privilèges sur le système.

4 Description

Plusieurs vulnérabilités, permettant à une personne malintentionnée d'élever ses privilèges, ont été découvertes dans IBM AIX :

- un dépassement de mémoire tampon est possible dans le programme privilégié *ndp* lorsque le service *netcd* est démarré ;

- si *RBAC (Role Based Access Control)* est utilisé et que l'utilisateur dispose de la permission *aix.network.config.tcpip*, un dépassement de mémoire débouchant sur une élévation de privilèges est possible via la commande *autoconf6* ;
- la suppression de n'importe quel fichier sur le système est possible via la commande *enq* si une file d'attente d'impression est définie dans */etc/qconfig* ;
- la commande *crontab* permet à un utilisateur disposant du droit *aix.system.config.cron* d'élèver ses privilèges pour l'édition de certains fichiers.

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 du 26 novembre 2008 :
http://aix.software.ibm.com/aix/efixes/security/aix61_advisory.asc

Gestion détaillée du document

01 décembre 2008 version initiale.