

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Faille dans la commande *enq* sous 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-2004-AVI-012>

---

### Gestion du document

Référence	CERTA-2004-AVI-012
Titre	Faille dans la commande <i>enq</i> sous AIX
Date de la première version	20 janvier 2004
Date de la dernière version	–
Source(s)	Avis 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 pour un utilisateur local.

## 2 Systèmes affectés

IBM AIX 4.3, 5.1 et 5.2.

## 3 Résumé

Un bogue de chaîne de format a été identifié dans la commande *enq* sous AIX. Il peut être exploité par un utilisateur local mal intentionné pour obtenir les privilèges *root*.

## 4 Description

La commande *enq* gère les files d'attente pour des ressources partagées, en particulier les imprimantes. Il est possible pour un utilisateur local mal intentionné d'obtenir les droits du programme, c'est-à-dire l'utilisateur *root* et le groupe *printq*.

## **5 Solution**

Mettre à jour le paquetage *bos.te.printers*, selon la version d'AIX :  
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1600.1>

## **6 Documentation**

Référence CVE CAN-2003-1018 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?CAN-2003-1018>

## **Gestion détaillée du document**

**20 janvier 2004** version initiale.