



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 septembre 2005
N° CERTA-2005-AVI-368

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des systèmes d'exploitation 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-2005-AVI-368>

Gestion du document

Référence	CERTA-2005-AVI-368
Titre	Vulnérabilité des systèmes d'exploitation AIX
Date de la première version	29 septembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM IY73850 et IY73814
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 ;
- exécution de code arbitraire.

2 Systèmes affectés

- AIX 5.2.0 ;
- AIX 5.3.0.

3 Résumé

Une vulnérabilité des systèmes AIX permet à un utilisateur local mal intentionné d'élever ses privilèges ou d'exécuter du code arbitraire.

4 Description

Une erreur de type débordement de tampon dans la commande `getconf` permet à un utilisateur local mal intentionné d'élever ses privilèges ou d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM IY73850 pour AIX 5.2.0 :
<http://www-1.ibm.com/support/docview.wss?uid=isgIY73850>
- Bulletin de sécurité IBM IY73814 pour AIX 5.3.0 :
<http://www-1.ibm.com/support/docview.wss?uid=isgIY73814>
- Référence CVE CAN-2005-3060 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3060>

Gestion détaillée du document

29 septembre 2005 version initiale.