

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'utilitaire AIX getconf

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-370>

Gestion du document

Référence	CERTA-2005-AVI-370
Titre	Vulnérabilité de l'utilitaire AIX getconf
Date de la première version	03 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Elévation des privilèges locaux.

2 Systèmes affectés

AIX versions 5.2 et 5.3.

3 Description

Une vulnérabilité de l'utilitaire AIX `getconf` a été découverte. Celle-ci permet à un utilisateur mal intentionné d'obtenir les privilèges de l'administrateur (`root`).

4 Contournement provisoire

Modifier les droits de `getconf` en enlevant le bit `suid` comme suit :

```
# chmod 555 /usr/bin/getconf
```

Le fait de modifier ce bit peut avoir des répercussions sur le système. Il conviendra donc d'exécuter cette commande en tant que super administrateur (*root*).

Il conviendra de même de vérifier que la modification a bien été prise en compte :

```
# ls -la /usr/bin/getconf
- -r-xr-xr-x 1 root bin 23430 Oct 03 2005 /usr/bin/getconf
```

5 Solution

Mettre à jour la version d'AIX comme indiqué sur le site de l'éditeur.

6 Documentation

- Site de l'éditeur :
<http://www-1.ibm.com/>
- Bulletin de sécurité et mises à jour :
<http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html>
- Référence CVE : CAN-2005-3060
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3060>

Gestion détaillée du document

03 octobre 2005 version initiale.