

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des systèmes AIX de IBM

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-075>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2005-AVI-075 |
| Titre | Multiples vulnérabilités des systèmes AIX de IBM |
| Date de la première version | 14 février 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité IBM du 9 février 2005 |
| Pièce(s) jointe(s) | |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Elévation de privilèges ;
- atteinte à la confidentialité des données ;
- exécution de code arbitraire.

2 Systèmes affectés

IBM AIX 5.X.

3 Résumé

Trois vulnérabilités présentes dans les systèmes AIX de IBM permettent à un utilisateur local mal intentionné d'exécuter du code arbitraire avec les privilèges du compte administrateur ou de porter atteinte à l'intégrité des données présentes sur le système.

4 Description

- La première vulnérabilité affecte la commande `lspath`. Elle permet à un utilisateur local mal intentionné de porter atteinte à la confidentialité des données (CAN-2005-0231) ;
- la seconde vulnérabilité, également de type débordement de la mémoire, est présente dans la commande `ipl_varyon`. Elle permet à un individu malveillant d'exécuter du code arbitraire avec les privilèges du compte administrateur (CAN-2005-0262) ;
- la dernière vulnérabilité, de type débordement de la mémoire, est présente dans la commande `netpmon`. Elle permet à un utilisateur local mal intentionné d'exécuter du code arbitraire avec les privilèges du compte administrateur (CAN-2005-0263).

5 Contournement provisoire

- Autoriser uniquement les personnes de confiance à accéder aux systèmes critiques ;
- restreindre le groupe `system` aux utilisateurs de confiance ;
- retirer de l'application `lspath` le drapeau `setuid` ;
- retirer de l'application `ipl_varyon` le drapeau `setuid` ;
- retirer de l'application `netpmon` le drapeau `setuid`.

6 Solution

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

7 Documentation

- Bulletin de sécurité de l'éditeur concernant AIX 5.1 :
<https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs?mode=1&heading=AIX51&topic=SECURITY&month>
- Bulletin de sécurité de l'éditeur concernant AIX 5.2 :
<https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs?mode=1&heading=AIX52&topic=SECURITY&month>
- Bulletin de sécurité de l'éditeur concernant AIX 5.3 :
<https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs?mode=1&heading=AIX51&topic=SECURITY&month>
- Correctif de l'éditeur `lspath` :
ftp://aix.software.ibm.com/aix/efixes/security/lspath_efix.tar.Z
- Correctif de l'éditeur `ipl_varyon` :
ftp://aix.software.ibm.com/aix/efixes/security/ipl_varyon_efix.tar.Z
- Correctif de l'éditeur `netpmon` :
ftp://aix.software.ibm.com/aix/efixes/security/netpmon_efix.tar.Z
- Bulletin de sécurité n° 195 d'iDEFENSE "IBM AIX `lspath` Local File Access Vulnerability" du 10 février 2005 :
<http://www.iddefense.com/application/poi/display?id=195&type=vulnerabilities>
- Bulletin de sécurité n° 196 d'iDEFENSE "IBM AIX `netpmonipl_varyon` Local Buffer Overflow Vulnerability" du 10 février 2005 :
<http://www.iddefense.com/application/poi/display?id=196&type=vulnerabilities>
- Bulletin de sécurité n° 197 d'iDEFENSE "IBM AIX `netpmon` Local Buffer Overflow Vulnerability" du 10 février 2005 :
<http://www.iddefense.com/application/poi/display?id=197&type=vulnerabilities>
- Référence CVE CAN-2005-0261 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0261>
- Référence CVE CAN-2005-0262 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0262>
- Référence CVE CAN-2005-0263 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0263>

Gestion détaillée du document

14 février 2005 version initiale.