

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-2007-AVI-464>

Gestion du document

Référence	CERTA-2007-AVI-464
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	31 octobre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité de 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

- Exécution de code arbitraire à distance ;
- atteinte à l'intégrité des données ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- IBM AIX 5.2 ;
- IBM AIX 5.3.

3 Résumé

De multiples vulnérabilités dans IBM AIX permettent à une personne malveillante d'exécuter du code arbitraire à distance, de porter atteinte à l'intégrité des données et de contourner la politique de sécurité.

4 Description

De multiples vulnérabilités ont été identifiées dans IBM AIX :

- Des vulnérabilités permettent à un individu malveillant l'exécution locale ou à distance de code arbitraire avec des privilèges d'administration ;
- une vulnérabilité permet une atteinte à l'intégrité des données et un contournement de la politique de sécurité.

5 Contournement provisoire

Des correctifs temporaires ont été mis à disposition par IBM pour certaines des vulnérabilités. Ces correctifs peuvent parfois avoir certains effets de bord, il est recommandé de les tester avant un déploiement sur des systèmes en production.

6 Solution

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

7 Documentation

- Bulletin de sécurité IBM IZ05065 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05065>
- Bulletin de sécurité IBM IZ05066 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05066>
- Bulletin de sécurité IBM IZ03055 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ03055>
- Bulletin de sécurité IBM IZ03061 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ03061>
- Bulletin de sécurité IBM IZ04832 du 18 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ04832>
- Bulletin de sécurité IBM IZ05017 du 29 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05017>
- Bulletin de sécurité IBM IZ05487 du 24 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05487>
- Bulletin de sécurité IBM IZ05488 du 24 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05488>
- Bulletin de sécurité IBM IZ05877 du 18 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05877>
- Bulletin de sécurité IBM IZ05971 du 18 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05971>
- Bulletin de sécurité IBM IZ05349 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05349>
- Bulletin de sécurité IBM IZ05129 du 25 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ05129>
- Bulletin de sécurité IBM IZ03054 du 29 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ03054>
- Bulletin de sécurité IBM IZ03060 du 29 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ03060>
- Bulletin de sécurité IBM IZ06648 du 29 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ06648>
- Bulletin de sécurité IBM IZ06001 du 29 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IZ06001>
- Référence CVE CVE-2007-4621 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4621>

- Référence CVE CVE-2007-4622 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4622>
- Référence CVE CVE-2007-4568 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4568>
- Référence CVE CVE-2007-4990 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4990>

Gestion détaillée du document

31 octobre 2007 version initiale.