Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 août 2007
N° CERTA-2007-AVI-352

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM AIX

Gestion du document

Référence	CERTA-2007-AVI-352
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	14 août 2007
Date de la dernière version	–
Source(s)	Correctifs fournis par IBM 5300-06-03 et 5200-10-02
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- IBM AIX 5.2 ;
- IBM AIX 5.3.

3 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation IBM AIX. Parmi celles-ci :

- un dysfonctionnement de la fonction `rmpvc` pourrait perturber le fonctionnement du système ;
- un débordement de tampon dans `lpd` de `bos.rte.printers` permettrait à un utilisateur local d'élever ses privilèges ;
- un débordement de tampon de `devices.common.IBM.atm.rte` permettrait à un utilisateur local d'élever ses privilèges ;

- un utilisateur dans le groupe `printq` peut élever ses privilèges à ceux d'administrateur, en trichant avec le programme `/usr/lib/lpd/pio/etc/pioinit` ;
- etc.

4 Solution

Se référer au bulletin d'IBM pour l'obtention des correctifs (Service Packs)(cf. section Documentation).

5 Documentation

- Service Pack 5300-06-03 pour IBM AIX 5.3, du 03 août 2007 :
  http://www14.software.ibm.com/webapp/set2/abl/fixinfo?release=53&b=5300-06-03
- Service Pack 5200-10-02 pour IBM, du 26 juillet 2007 :
  http://www14.software.ibm.com/webapp/set2/abl/fixinfo?release=52&b=5200-10-02
- Bulletin de sécurité IBM IY98395 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IY98395
- Bulletin de sécurité IBM IZ00139 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ00139
- Bulletin de sécurité IBM IZ00149 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ00149
- Bulletin de sécurité IBM IZ00154 du 27 juillet 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ00154
- Bulletin de sécurité IBM IZ01122 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ01122
- Bulletin de sécurité IBM IZ01433 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ01433
- Bulletin de sécurité IBM IZ1437 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ1437
- Bulletin de sécurité IBM IZ01535 du 03 août 2007 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ01535
- Référence CVE CVE-2007-3333 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3333
- Référence CVE CVE-2007-4003 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4003
- Référence CVE CVE-2007-4004 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4004
- Référence CVE CVE-2007-4228 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4228
- Référence CVE CVE-2007-4236 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4236
- Référence CVE CVE-2007-4237 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4237
- Référence CVE CVE-2007-4238 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4238

Gestion détaillée du document

14 août 2007 version initiale.