Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mai 2008
N° CERTA-2008-AVI-267

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'AIX

Gestion du document

Référence	CERTA-2008-AVI-267
Titre	Multiples vulnérabilités d'AIX
Date de la première version	22 mai 2008
Date de la dernière version	–
Source(s)	Bulletin IBM du 21 mai 2008
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 ;
- exécution de code arbitraire ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

IBM AIX, version 5.2, 5.3 et 6.1.

3 Résumé

Plusieurs vulnérabilités affectent *IBM AIX* et permettent, en particulier, à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent *IBM AIX* :

- un débordement de mémoire est possible dans une fonction d'impression et utilisable par un utilisateur malveillant pour exécuter du code arbitraire avec les droits d'administration du système ;
- un autre débordement de mémoire concerne le noyau et permet de provoquer une arrêt inopiné ou une exécution de code arbitraire à distance ;
- un débordement de mémoire est possible dans la fonction `errpt` et permet à un utilisateur malveillant d'exécuter du code arbitraire avec les droits d'administration du système ;
- deux vulnérabilités concernent OpenSSH et permettent à un utilisateur malveillant de contourner la politique de sécurité ;
- le service FTP peut révéler des données sensibles à un utilisateur malveillant sans nécessiter l'authentification de ce dernier ;
- une erreur de gestion des variables d'environnement dans `iostat` est exploitable par un utilisateur malveillant local pour exécuter du code arbitraire avec les droits d'administration du système.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM du 19 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/pioout_advisory.asc
- Bulletin de sécurité IBM du 21 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/unix_advisory.asc
- Bulletin de sécurité IBM du 21 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/errpt_advisory.asc
- Bulletin de sécurité IBM du 21 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/ssh_advisory.asc
- Bulletin de sécurité IBM du 21 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/ftpd_advisory.asc
- Bulletin de sécurité IBM du 21 mai 2008 :
  http://aix.software.ibm.com/aix/efixes/security/iostat_advisory.asc
- Référence CVE CVE-1999-0201 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0201
- Référence CVE CVE-2007-5764 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5764
- Référence CVE CVE-2008-1483 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1483
- Référence CVE CVE-2008-1657 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1657

Gestion détaillée du document

22 mai 2008 version initiale.