Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2008
N° CERTA-2008-AVI-135

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-2008-AVI-135

Gestion du document

Référence	CERTA-2008-AVI-135
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	13 mars 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM du 11 mars 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 ;
- déni de service ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- IBM AIX 5.2 ;
- IBM AIX 5.3 ;
- IBM AIX 6.1.

3 Résumé

De multiples vulnérabilités affectent IBM AIX et permettent à un utilisateur local d'exécuter du code arbitraire, de réaliser un déni de service, de contourner la politique de sécurité ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités affectent `IBM` ; ces vulnérabilités concernent :

- le noyaux AIX : plusieurs vulnérabilités affectant la gestion des processus 64-bit, la gestion des *Volume Group*, la gestion des droits, la gestion des liens, les appels système et la commande *ProbeVue* permettent à un utilisateur local d'exécuter du code arbitraire, de réaliser un déni de service, de contourner la politique de sécurité ou d'élever ses privilèges ;
- la famille de commandes *nddstat* : un défaut de contrôle de certaines variables permet à un utilisateur local d'exécuter du code arbitraire en exploitant cette vulnérabilité ;
- la commande *lsmcode* : un défaut de contrôle de certaines variables permet à un utilisateur local d'exécuter du code arbitraire en exploitant cette vulnérabilité ;
- la commande *reboot* : une vulnérabilité permet à un utilisateur local, ayant les privilèges nécessaires pour exécuter cette commande, d'exécuter du code arbitraire via un débordement de mémoire.

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 IZ16992 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ16992
- Bulletin de sécurité IBM IZ17111 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ17111
- Bulletin de sécurité IBM IZ11820 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ11820
- Bulletin de sécurité IBM IZ12794 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ12794
- Bulletin de sécurité IBM IZ16991 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ16991
- Bulletin de sécurité IBM IZ17058 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ17058
- Bulletin de sécurité IBM IZ17059 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ17059
- Bulletin de sécurité IBM IZ16975 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ16975
- Bulletin de sécurité IBM IZ15276 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15276
- Bulletin de sécurité IBM IZ15100 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15100
- Bulletin de sécurité IBM IZ15057 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15057
- Bulletin de sécurité IBM IZ15277 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15277
- Bulletin de sécurité IBM IZ15479 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15479
- Bulletin de sécurité IBM IZ15480 du 11 mars 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=isg1IZ15480

Gestion détaillée du document

13 mars 2008 version initiale.