



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 mai 2010
N° CERTA-2010-AVI-224

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2010-AVI-224>

Gestion du document

Référence	CERTA-2010-AVI-224
Titre	Vulnérabilité dans IBM AIX
Date de la première version	21 mai 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM du 18 mai 2010
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.

2 Systèmes affectés

- IBM AIX 5.x et 6.x ;
- IBM VIOS 1.x et 2.x.

3 Résumé

Une vulnérabilité dans un service de systèmes d'exploitation IBM est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance.

4 Description

Un débordement d'entier est présent dans le service `rpc.pcnfsd`. Il est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletins de sécurité IBM du 18 mai 2010 :
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ73874>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ73757>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ73681>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ73590>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ75465>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ75440>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ75369>
 - <http://www-01.ibm.com/support/docview.wss?uid=isg1IZ73599>
- Référence CVE CVE-2010-1039 :
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1039>

Gestion détaillée du document

21 mai 2010 version initiale.