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 septembre 2010
N° CERTA-2010-AVI-428

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans IBM AIX

Gestion du document

Référence	CERTA-2010-AVI-428
Titre	Vulnérabilités dans IBM AIX
Date de la première version	14 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM du 13 septembre 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

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

2 Systèmes affectés

- *AIX 5.3* pour le contournement de la politique de sécurité ;
- *AIX 6.1*, *AIX 5.3* et versions antérieures, *VIOS* versions 1.5 et 2.1 pour l'élévation de privilèges.

3 Résumé

Un utilisateur authentifié malveillant peut exploiter plusieurs vulnérabilités dans *IBM AIX* pour élever ses privilèges et supprimer des informations auxquelles il ne devrait pas avoir accès.

4 Description

Deux vulnérabilités touchent ces produits *IBM* :

- un débordement de tampon dans le programme */usr/esa/sbin/sa_snap* permet à un attaquant d'élever ses privilèges ;

– un attaquant peut contourner la politique de sécurité et supprimer des fichiers sensibles via une erreur non spécifiée par l'éditeur.

Ces deux vulnérabilités, pour être exploitables, requièrent que l'attaquant possède les privilèges « system group user ».

5 Solution

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

6 Documentation

– Bulletin de sécurité IBM du 13 septembre 2010
http://aix.software.ibm.com/aix/efixes/security/sa_snap_advisory.asc

Gestion détaillée du document

14 septembre 2010 version initiale.