Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2005
N° CERTA-2005-AVI-064

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des systèmes AIX de IBM

Gestion du document

Référence	CERTA-2005-AVI-064
Titre	Vulnérabilité des systèmes AIX de IBM
Date de la première version	10 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité IY67519 de IBM du 08 février 2005 Bulletin de sécirité iDEFENSE IBM AIX auditselect local format String Vulnerability
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Elévation de privilèges.

2 Systèmes affectés

IBM AIX 5.3 et versions antérieures.

3 Description

Une vulnérabilité de type chaine de format dans l'application `auditselect` permet à un utilisateur local mal intentionné qui fait partie groupe `audit` afin d'exécuter du code arbitraire avec les privilèges du compte `root`.

4 Contournement provisoire

– Autoriser uniquement les personnes de confiance à accéder aux systèmes critiques ;
– restreindre le groupe `audit` aux adminsitrateurs systèmes ;

– retirer de l'application `auditselect` le drapeau `setuid`.

5 Solution

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

6 Documentation

– Bulletin de sécurité d'IBM :
http://www-1.ibm.com/support/docview.wss?uid=isg1IY67519
– Bulletin de sécurité n193 d'iDEFENSE "IBM AIX auditselect local format String Vulnerability" du 08 février 2005 :
http://www.idefense.com/application/poi/display?id=193&type=vulnerabilities
– Référence CVE CAN-2005-0250 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0250

Gestion détaillée du document

10 février 2005 version initiale.