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 février 2003
N° CERTA-2003-AVI-022

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque libIM.a sous IBM AIX

Gestion du document

Référence	CERTA-2003-AVI-022
Titre	Vulnérabilité de la bibliothèque libIM.a sous IBM AIX
Date de la première version	13 février 2003
Date de la dernière version	–
Source(s)	Avis de sécurité de iDefense du 12.02.03
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 en local ;
- élévation de privilèges.

2 Systèmes affectés

IBM AIX versions 4.3.3, 5.1.0 et 5.2.0.

3 Résumé

Un débordement de tampon dans la bibliothèque libIM.a permet à un utilisateur local mal intentionné d'exécuter du code arbitraire avec les droits de l'application faisant appel à cette bibliothèque.

4 Description

La bibliothèque système libIM.a est utilisée pour l'internationalisation (`National Language Support` ou `NLS`). Un débordement de tampon dans la bibliothèque libIM.a permet à un utilisateur `local` mal intentionné

d'exécuter du code arbitraire avec les droits de l'application faisant appel à cette bibliothèque. Si l'application possède le drapeau `setuid root`, l'utilisateur local mal intentionné peut exécuter du code arbitraire avec les droits `root`.

5 Contournement provisoire

Appliquer le correctif provisoire fournit par IBM (cf. section documentation). Vérifier l'empreinte MD5 avant tout utilisation des correctifs.

6 Solution

IBM va mettre à disposition les correctifs suivants :

- Pour IBM AIX 4.3.3, correctif IY40307 ;
- pour IBM AIX 5.1.0, correctif IY40317 ;
- pour IBM AIX 5.2.0, correctif IY40320.

7 Documentation

- Avis de sécurité de iDefense du 12.02.03 :
  http://www.idefense.com/advisory/02.12.03.txt
- Site FTP de IBM de téléchargement du correctif provisoire :
  ftp://aix.software.ibm.com/aix/efixes/security/libIM_efix.tar.Z

Gestion détaillée du document

13 février 2003 version initiale.