



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2011
N° CERTA-2011-AVI-702

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2011-AVI-702>

Gestion du document

Référence	CERTA-2011-AVI-702
Titre	Vulnérabilités dans AIX
Date de la première version	16 décembre 2011
Date de la dernière version	–
Sources	Bulletins de sécurité IBM AIX des 14 et 15 décembre 2012
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 ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

AIX 5.x, 6.x et 7.x.

3 Résumé

Plusieurs vulnérabilités dans AIX permettent à un utilisateur malveillant d'exécuter du code arbitraire ou de modifier des données.

4 Description

Plusieurs vulnérabilités affectent AIX :

- deux d'entre elles résident dans le serveur X et permettent à un utilisateur malveillant de corrompre la mémoire et d'exécuter du code arbitraire ;

- un autre problème permet à un utilisateur malveillant de détruire des fichiers vitaux du système ou d'utiliser des logiciels sur des fichiers non autorisés.

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 AIX du 14 décembre 2011 :
http://aix.software.ibm.com/aix/efixes/security/xorg_advisory.asc
- Bulletin de sécurité IBM AIX du 15 décembre 2011 :
http://aix.software.ibm.com/aix/efixes/security/invscout_advisory2.asc
- Référence CVE CVE-2007-6427 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6427>
- Référence CVE CVE-2007-6429 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6429>
- Référence CVE CVE-2011-1384 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1384>

Gestion détaillée du document

16 décembre 2011 version initiale.