

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-2010-AVI-269>

Gestion du document

Référence	CERTA-2010-AVI-269
Titre	Vulnérabilités dans AIX
Date de la première version	17 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM du 16 juin 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.

2 Systèmes affectés

AIX 5.2, 5.3 et 6.1.

3 Résumé

Deux vulnérabilités dans la distribution AIX d'OpenSSH permettent à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

Deux vulnérabilités dans la distribution d'OpenSSH faite avec AIX ont été publiées :

- une attaque par interposition (*man in the middle*) est possible quand l'option de configuration du serveur SSH `X11USELOCALHOST` est positionnée à la valeur `no` ;
- dans la configuration proposée en standard, un attaquant peut découvrir 32 bits de chaque bloc de données chiffré dans une connexion SSH.

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 16 juin 2010 :

<http://www14.software.ibm.com/webapp/set2/subscriptions/pqcvmjd?mode=18&ID=5118&myns=paix52&mync=E>

Gestion détaillée du document

17 juin 2010 version initiale.