

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM 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-2009-AVI-556>

Gestion du document

Référence	CERTA-2009-AVI-556-001
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	21 décembre 2009
Date de la dernière version	24 décembre 2009
Source(s)	Bulletins de sécurité IBM du 16 décembre 2009
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

Élévation de privilèges.

2 Systèmes affectés

IBM AIX 6.x.

3 Résumé

Plusieurs vulnérabilités présentes dans *IBM AIX* permettent à un utilisateur local malintentionné d'élever ses privilèges.

4 Description

Deux vulnérabilités sont présentes dans le système d'exploitation *IBM AIX* :

- la première est relative à une faille de type débordement de mémoire dans la commande *qosmod* ;
- la seconde concerne le même type de vulnérabilité dans la commande *qoslist*.

L'exploitation de ces deux vulnérabilités permet à un utilisateur local malintentionné d'élever ses privilèges.

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 IZ66917 du 16 décembre 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=isg1IZ66917>
- Bulletin de sécurité IBM IZ66918 du 16 décembre 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=isg1IZ66918>
- Bulletin de sécurité IBM IZ66966 du 16 décembre 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=isg1IZ66966>
- Bulletin de sécurité IBM IZ66967 du 16 décembre 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=isg1IZ66967>
- Référence CVE CVE-2009-4361 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4361>
- Référence CVE CVE-2009-4362 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4362>

Gestion détaillée du document

21 décembre 2009 version initiale.

24 décembre 2009 ajout des références CVE.