Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 octobre 2006
N° CERTA-2006-AVI-415

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM AIX

Gestion du document

Référence	CERTA-2006-AVI-415
Titre	Multiples vulnérabilités dans IBM AIX
Date de la première version	03 octobre 2006
Date de la dernière version	–
Source(s)	Avis de sécurité IBM AIX
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

- Déni de service ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- IBM AIX 5.2.0
- IBM AIX 5.3.0

3 Description

De multiples vulnérabilités ont été identifiées dans le système d'exploitation IBM AIX. Elles permettraient à un utilisateur malveillant local au système vulnérable d'élever ses privilèges à ceux de l'administrateur (*root*), voire de modifier des données ou de provoquer un déni de service. Parmi ces vulnérabilités :

- la commande `mkvg` ne faisant pas appel aux chemins absolus vers certaines fonctions ;
- une erreur non précisée dans `named8`, un serveur de noms de domaines `DNS` ;

- une mauvaise manipulation des fichiers par la commande `rdist`, servant à distribuer des copies de fichiers à plusieurs hôtes ;
- une mauvaise manipulation de la base de données par l'utilitaire `Inventory Scout`, permettant de lister entre autres les éléments matériels du système ;
- une erreur non précisée dans la commande `utape` associée au mode `Diagnostics` ;
- une mauvaise manipulation des paramètres fournis à la commande `cfgmgr`, pouvant provoquer un débordement de mémoire ;
- une erreur non précisée dans `xlock`, commande qui permet de verrouiller l'écran, et pouvant être exploitée pour provoquer un débordement de tampon et exécuter des commandes avec les droits de l'administrateur.

4 Solution

Se référer aux différents bulletins de sécurité d'IBM pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité IBM IY88820 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88820
- Bulletin de sécurité IBM IY88818 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88818
- Bulletin de sécurité IBM IY88566 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88566
- Bulletin de sécurité IBM IY88615 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88615
- Bulletin de sécurité IBM IY89512 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY89512
- Bulletin de sécurité IBM IY89434 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY89434
- Bulletin de sécurité IBM IY88641 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88641
- Bulletin de sécurité IBM IY88642 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88642
- Bulletin de sécurité IBM IY88735 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88735
- Bulletin de sécurité IBM IY88688 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88688
- Bulletin de sécurité IBM IY88687 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88687
- Bulletin de sécurité IBM IY88565 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88565
- Bulletin de sécurité IBM IY88614 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88614
- Bulletin de sécurité IBM IY88722 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88722
- Bulletin de sécurité IBM IY88699 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY88699
- Bulletin de sécurité IBM IY87943 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY87943
- Bulletin de sécurité IBM IY87894 du 14 septembre 2006 : http://www-1.ibm.com/support/docview.wss?uid=isg1IY87894
- Référence CVE CVE-2006-4416 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4416

- Référence CVE CVE-2006-5002 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5002
- Référence CVE CVE-2006-5003 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5003
- Référence CVE CVE-2006-5004 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5004
- Référence CVE CVE-2006-5005 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5005
- Référence CVE CVE-2006-5006 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5006
- Référence CVE CVE-2006-5007 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5007
- Référence CVE CVE-2006-5008 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5008
- Référence CVE CVE-2006-5009 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5009
- Référence CVE CVS-2006-5011 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVS-2006-5011

Gestion détaillée du document

03 octobre 2006 version initiale.