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 janvier 2006
N° CERTA-2005-AVI-500-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans VMware

Gestion du document

Référence	CERTA-2005-AVI-500-001
Titre	Vulnérabilité dans VMware
Date de la première version	22 décembre 2005
Date de la dernière version	16 janvier 2006
Source(s)	Bulletin de sécurité VMware
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

Accès au système hôte.

2 Systèmes affectés

- VMware ACE 1.x ;
- VMware GSX Server 1.x ;
- VMware GSX Server 2.x ;
- VMware GSX Server 3.x ;
- VMware Player 1.x ;
- VMware Workstation 2.x ;
- VMware Workstation 3.x ;
- VMware Workstation 4.x ;
- VMware Workstation 5..x

3 Résumé

Une vulnérabilité dans le service de traduction d'adresses de l'émulateur VMware peut être exploitée par un utilisateur mal intentionné pour accèder au système hébergeant la machine virtuelle.

4 Description

Une vulnérabilité est présente dans le service de traduction d'adresses : `vmnat.exe` sous windows et `vmnet-natd` sous linux.

Cette vulnérabilité est due à un problème dans le traitement des requêtes FTP. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné pour accéder à la machine hébergeant la machine virtuelle.

5 Solution

Mettre à jour avec les nouvelles versions de VMware.

6 Documentation

- Site Internet de VMware :
  http://www.vmware.com
- Bulletin de sécurité VMware :
  http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=2002
- Bulletin de sécurité Gentoo GLSA 200601-04 du 07 janvier 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200601-04.xml
- Référence CVE CVE-2005-4459 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4459

Gestion détaillée du document

22 décembre 2005 version initiale.
16 janvier 2006 ajout de la référence au bulletin de sécurité Gentoo et la référence CVE.