

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits VMware

---

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-2008-AVI-291>

---

### Gestion du document

Référence	CERTA-2008-AVI-291
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	05 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-0009 du 04 juin 2008
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMware ESX Server 2.x ;
- VMware ESX Server 3.x ;
- VMware ACE 1.x ;
- VMware Player 1.x ;
- VMware Server 1.x ;
- VMware VIX API 1.x ;
- VMware Workstation 5.x ;

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans les produits de virtualisation VMware. Ces vulnérabilités peuvent être exploitées en local afin de contourner la politique de sécurité ou d'obtenir des privilèges élevés.

## 4 Description

Quatres vulnérabilités ont été découvertes dans les produits VMware :

- la première est présente au niveau du pilote HGFS.sys, installé par l'ensemble d'outils VMTools. L'exploitation de cette vulnérabilité permet d'exécuter du code arbitraire sous des privilèges élevés sur une machine virtuelle (*guest*) Windows ;
- la deuxième est due à une erreur au niveau du démon `vmware-authd`. Elle peut être exploitée sur une machine hôte Linux afin d'obtenir des privilèges élevés ;
- la troisième résulte d'une erreur dans le service de gestion *Openwsman*. Cette vulnérabilité peut être exploitée afin d'obtenir les privilèges administrateur (*root*) sur un hôte Linux.
- la quatrième vulnérabilité résulte de plusieurs erreurs aux limites dans VMware VIX API, entraînant un certain nombre de possibilités de débordement d'allocation mémoire.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité VMware VMSA-2008-0009 du 04 juin 2008 :  
<http://www.vmware.com/security/advisories/VMSA-2008-0009.html>
- Référence CVE CVE-2007-5671 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5671>
- Référence CVE CVE-2008-0967 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0967>
- Référence CVE CVE-2008-2097 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2097>
- Référence CVE CVE-2008-2100 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2100>

## Gestion détaillée du document

**05 juin 2008** version initiale.