

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans VMware ESX Server

---

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-103>

---

### Gestion du document

Référence	CERTA-2008-AVI-103-001
Titre	Multiples vulnérabilités dans VMware ESX Server
Date de la première version	22 février 2008
Date de la dernière version	28 février 2008
Source(s)	Bulletin de sécurité VMware VMSA-2008-0003 du 04 février 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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- élévation de privilèges ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- VMware ESX Server 2.x ;
- VMware ESX Server 3.x.

## 3 Résumé

Plusieurs vulnérabilités dans VMware ESX Server permettent à une personne malintentionnée d'élever ses privilèges, d'atteindre à la confidentialité des données, d'exécuter du code arbitraire ou de provoquer un déni de service.

## 4 Description

Plusieurs vulnérabilités dans VMware ESX Server ont été découvertes :

- une erreur dans le pilote *aacraid SCSI* permet à un utilisateur local de provoquer un déni de service ou une élévation de privilèges ;
- une vulnérabilité dans Samba permet à une personne malveillante ayant accès à la console de service de provoquer un déni de service ou d'exécuter du code arbitraire à distance ;
- plusieurs vulnérabilités dans le module *python* permettent de provoquer un déni de service, d'exécuter du code arbitraire ou d'atteindre à la confidentialité des données.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité VMware VMSA-2008-0003 du 04 février 2008 :  
<http://www.vmware.com/security/advisories/VMSA-2008-0003.html>
- Référence CVE CVE-2006-7228 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7228>
- Référence CVE CVE-2007-2052 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2052>
- Référence CVE CVE-2007-4308 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4308>
- Référence CVE CVE-2007-4965 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4965>
- Référence CVE CVE-2007-6015 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6015>

## Gestion détaillée du document

**22 février 2008** version initiale.

**28 février 2008** correction du lien vers le bulletin de sécurité VMware.