

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-008>

---

### Gestion du document

Référence	CERTA-2008-AVI-008
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	08 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMWare VMSA-2008-0001 du 07 janvier 2008 Bulletin de sécurité VMWare VMSA-2008-0002 du 07 janvier 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 ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMWare ESX Server 2.0.x ;
- VMWare ESX Server 3.0.x ;
- VirtualCenter Management Server 2.

## 3 Résumé

De multiples vulnérabilités sur *VMWare ESX Server* et *VirtualCenter Management Server* permettent notamment à une personne malintentionnée distante d'exécuter du code arbitraire.

## 4 Description

De multiples vulnérabilités existent sur *VMWare ESX Server*. Celles-ci concernent des modules ou logiciels utilisés par le serveur et récemment mis à jour : *OpenPegasus*, *Tomcat*, *Samba*, *OpenSSL*, *JRE*, *util-linux*, et *Perl*. Certaines de ces failles permettent notamment à une personne malintentionnée distante d'exécuter du code arbitraire.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité VMWare VMSA-2008-0001 du 07 janvier 2008 :  
<http://lists.vmware.com/pipermail/security-announce/2008/000002.html>
- Bulletin de sécurité VMWare VMSA-2008-0002 du 07 janvier 2008 :  
<http://lists.vmware.com/pipermail/security-announce/2008/000003.html>
- Référence CVE CVE-2005-2090 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2090>
- Référence CVE CVE-2006-7195 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7195>
- Référence CVE CVE-2007-0450 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0450>
- Référence CVE CVE-2007-3004 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3004>
- Référence CVE CVE-2007-5360 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5360>
- Référence CVE CVE-2007-5398 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5398>
- Référence CVE CVE-2007-4572 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4572>
- Référence CVE CVE-2007-5191 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5191>
- Référence CVE CVE-2007-5116 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5116>
- Référence CVE CVE-2007-3108 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3108>
- Référence CVE CVE-2007-5135 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5135>

## Gestion détaillée du document

**08 janvier 2008** version initiale.