

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-2010-AVI-162>

---

### Gestion du document

Référence	CERTA-2010-AVI-162
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	09 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0007 du 09 avril 2010
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 ;
- exécution de code arbitraire ;
- déni de service ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMware Workstation 7.x et 6.x ;
- VMware Player 3.x et 2.x ;
- VMware ACE 2.x ;
- VMware Server 2.x ;
- VMware Fusion 3.x et 2.x ;
- VMware VIX API ;
- VMware ESX et ESXi ;

### 3 Résumé

De multiples vulnérabilités affectant les produits VMware ont été publiées. Elles permettent à un utilisateur malveillant d'effectuer diverses atteintes à la sécurité du système vulnérable.

### 4 Description

De multiples vulnérabilités affectant les produits VMware ont été publiées. Elles permettent à un utilisateur malveillant d'effectuer diverses atteintes à la sécurité du système vulnérable :

- exécution de code arbitraire à distance dans le contexte de l'utilisateur connecté ;
- exécution de code arbitraire ;
- déni de service local ;
- atteinte à la confidentialité des données par utilisation de la pile réseau virtuelle ;
- élévation de privilèges sur des systèmes Windows.

### 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-2010-0007 du 09 avril 2010 :  
<http://lists.vmware.com/pipermail/security-announce/2010/000090.html>
- Référence CVE CVE-2009-1564 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1564>
- Référence CVE CVE-2009-1565 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1565>
- Référence CVE CVE-2009-2042 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2042>
- Référence CVE CVE-2009-3707 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3707>
- Référence CVE CVE-2009-3732 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3732>
- Référence CVE CVE-2010-1138 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1138>
- Référence CVE CVE-2010-1139 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1139>
- Référence CVE CVE-2009-1140 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1140>
- Référence CVE CVE-2009-1141 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1141>
- Référence CVE CVE-2009-1142 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1142>

### Gestion détaillée du document

09 avril 2010 version initiale.