

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités des 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-2009-AVI-464>

---

### Gestion du document

Référence	CERTA-2009-AVI-464
Titre	Multiples vulnérabilités des produits VMware
Date de la première version	30 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2009-0015 du 27 octobre 2009
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

- Atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMware Workstation version 6.5.2 et versions antérieures ;
- VMware Player version 2.5.2 et versions antérieures ;
- VMware ACE version 2.5.2 et versions antérieures ;
- VMware Server version 2.0.1 et versions antérieures ;
- VMware Server version 1.0.9 et versions antérieures ;
- VMware Fusion version 2.0.5 et versions antérieures ;
- VMware ESXi version 4.0 sans la mise à jour ESXi400-200909401-BG ;
- VMware ESXi version 3.5 sans les mises à jour ESXe350-200910401-I-SG et ESXe350-200901401-I-SG ;
- VMware ESX version 4.0 sans la mise à jour ESX400-200909401-BG ;
- VMware ESX version 3.5 sans les mises à jour ESX350-200910401-SG et ESX350-200901401-SG ;
- VMware ESX version 3.0.3 sans les mises à jour ESX303-200910401-SG et ESX350-200901401-SG ;
- VMware ESX version 2.5.5 sans la mise à jour numéro 15 ;

### 3 Résumé

Deux vulnérabilités permettant d'accéder à des informations sensibles et d'augmenter ses privilèges ont été découvertes dans VMware.

### 4 Description

Deux vulnérabilités ont été découvertes dans les produits VMware :

- la première est due à une mauvaise gestion des exceptions et permet à un utilisateur malintentionné d'élever ses privilèges ;
- la seconde consiste en une vulnérabilité de type *directory traversal* et permet à un utilisateur malintentionné d'accéder à des fichiers stockés sur la machine hôte.

### 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 numéro VMSA-2009-0015 du 27 octobre 2009 :  
<http://www.vmware.com/security/advisories/VMSA-2009-0015.html>
- Référence CVE CVE-2009-2267 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2267>
- Référence CVE CVE-2009-3733 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3733>

## Gestion détaillée du document

30 octobre 2009 version initiale.