



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 06 juin 2011  
N° CERTA-2011-AVI-330

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-2011-AVI-330>

---

### Gestion du document

Référence	CERTA-2011-AVI-330
Titre	Multiples vulnérabilités dans les produits VMWare
Date de la première version	06 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2011-0009 du 06 juin 2011
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMWare Workstation versions 7.1.3 et antérieures ;
- VMWare Player versions 3.1.3 et antérieures ;
- VMWare Fusion versions 3.1.2 et antérieures ;
- ESXi 4.1 sans le correctif ESXi410-201104402-BG ;
- ESXi 4.0 sans le correctif ESXi400-201104402-BG ;
- ESXi 3.5 sans les correctifs ESXe350-201105401-SG et ESXe350-201105402-T-SG ;
- ESXi 4.1 sans le correctif ESX410-201104401-BG ;
- ESXi 4.0 sans le correctif ESX400-201104401-BG ;
- ESXi 3.5 sans les correctifs ESX350-201105401-SG, ESXe350-201105404-SG et ESXe350-201105406-SG ;

### 3 Résumé

De nombreuses vulnérabilités ont été corrigées dans les produits VMWare, dont certaines peuvent permettre l'exécution de code arbitraire à distance.

### 4 Description

De nombreuses vulnérabilités ont été corrigées dans les produits VMWare :

- une vulnérabilité dans le pilote pour les cartes Intel PRO/1000 sous Linux, qui peut être exploitée pour contourner les filtres réseaux ;
- plusieurs vulnérabilités dans des composants tiers du serveur ESX permettent à un utilisateur local malveillant d'élever ses privilèges, à un attaquant sous certaines conditions d'exécuter du code arbitraire à distance, et à un attaquant de créer des dénis de service localement ou à distance ;
- plusieurs vulnérabilités dans le système de fichiers Host Guest (HGFS) pour les systèmes Unix peuvent être exploitées par un attaquant dans la machine cliente pour obtenir des informations sur l'existence de fichiers sur la machine hôte, et pour élever ses privilèges (notamment par un accès concurrentiel type "Race Condition" en montant un répertoire) ;
- une vulnérabilité dans les contrôles ActiveX du client VI permet à un attaquant d'exécuter du code arbitraire à distance à l'aide d'un site Web spécialement conçu.

### 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-2011-0009 du 06 juin 2011 :  
<http://www.vmware.com/security/advisories/VMSA-2011-0009.html>
- Référence CVE CVE-2009-3080 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3080>
- Référence CVE CVE-2009-4536 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4536>
- Référence CVE CVE-2010-1188 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1188>
- Référence CVE CVE-2010-2240 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2240>
- Référence CVE CVE-2011-2146 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2146>
- Référence CVE CVE-2011-1787 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1787>
- Référence CVE CVE-2011-2145 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2145>
- Référence CVE CVE-2011-2217 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2217>

### Gestion détaillée du document

06 juin 2011 version initiale.