

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans VMware ESX

---

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-008>

---

### Gestion du document

Référence	CERTA-2010-AVI-008
Titre	Multiples vulnérabilités dans VMware ESX
Date de la première version	08 janvier 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0001 du 06 janvier 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

VMware ESX 4.0 sans le correctif ESX400-200912403-SG.

## 3 Résumé

Plusieurs vulnérabilités dans VMware ESX permettent, entre autre, à une personne malintentionnée d'exécuter du code arbitraire à distance

## 4 Description

De multiples vulnérabilités, non documentées, dans VMware ESX permettent, entre autre, à une personne distante malintentionnée d'exécuter du code arbitraire.

## 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-2010-0001 du 06 janvier 2010 :  
<http://lists.vmware.com/pipermail/security-announce/2010/000075.html>
- Référence CVE CVE-2009-1563 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1563>
- Référence CVE CVE-2009-2404 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2404>
- Référence CVE CVE-2009-2408 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408>
- Référence CVE CVE-2009-2409 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409>
- Référence CVE CVE-2009-3274 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3274>
- Référence CVE CVE-2009-3370 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3370>
- Référence CVE CVE-2009-3372 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3372>
- Référence CVE CVE-2009-3373 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3373>
- Référence CVE CVE-2009-3374 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3374>
- Référence CVE CVE-2009-3375 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3375>
- Référence CVE CVE-2009-3376 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3376>
- Référence CVE CVE-2009-3380 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3380>
- Référence CVE CVE-2009-3382 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3382>

## Gestion détaillée du document

**08 janvier 2010** version initiale.