



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 mars 2010  
N° CERTA-2010-AVI-106

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-106>

---

### Gestion du document

Référence	CERTA-2010-AVI-106
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	04 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware du 03 mars 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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- VMware ESX 4.0 sans les patches SX400-201002404-SG, SX400-201002406-SG, SX400-201002407-SG ;
- VMware ESX 3.5 ;
- VMware ESX 3.0.3 ;
- VMware ESX 2.5.5 ;
- VMware vMA 4.0 sans le patch 3.

### 3 Résumé

Plusieurs vulnérabilités découvertes dans les produits VMware peuvent être exploitées à distance par un utilisateur malintentionné afin de compromettre le système ou d'entraver son bon fonctionnement.

### 4 Description

Les vulnérabilités présentes dans les produits VMware peuvent être exploitées afin de porter atteinte à l'intégrité et à la confidentialité des données, de réaliser un déni de service, d'injecter et d'exécuter indirectement du code arbitraire, d'élever ses privilèges ou 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 du 03 mars 2010 :  
<http://lists.vmware.com/pipermail/security-announce/2010/000082.html>
- Référence CVE CVE-2009-2905 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2905>
- Référence CVE CVE-2008-4552 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4552>
- Référence CVE CVE-2008-4316 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4316>
- Référence CVE CVE-2009-1377 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1377>
- Référence CVE CVE-2009-1378 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1378>
- Référence CVE CVE-2009-1379 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1379>
- Référence CVE CVE-2009-1386 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1386>
- Référence CVE CVE-2009-1387 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1387>
- Référence CVE CVE-2009-0590 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0590>
- Référence CVE CVE-2009-4022 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4022>
- Référence CVE CVE-2009-3560 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3560>
- Référence CVE CVE-2009-3720 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3720>
- Référence CVE CVE-2009-2904 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2904>
- Référence CVE CVE-2009-3563 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3563>
- Référence CVE CVE-2009-2695 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2695>
- Référence CVE CVE-2009-2849 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2849>
- Référence CVE CVE-2009-2695 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2695>

- Référence CVE CVE-2009-2908 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2908>
- Référence CVE CVE-2009-3228 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3228>
- Référence CVE CVE-2009-3286 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3286>
- Référence CVE CVE-2009-3547 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3547>
- Référence CVE CVE-2009-3613 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3613>
- Référence CVE CVE-2009-3612 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3612>
- Référence CVE CVE-2009-3620 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3620>
- Référence CVE CVE-2009-3621 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3621>
- Référence CVE CVE-2009-3726 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3726>
- Référence CVE CVE-2009-3916 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3916>
- Référence CVE CVE-2009-1189 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1189>
- Référence CVE CVE-2009-0115 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0115>

## **Gestion détaillée du document**

**04 mars 2010** version initiale.