



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 mai 2007  
N° CERTA-2006-AVI-501-001

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-2006-AVI-501>

---

### Gestion du document

Référence	CERTA-2006-AVI-501-001
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	15 novembre 2006
Date de la dernière version	29 mai 2007
Source(s)	Bulletins de sécurité VMware du 13 Novembre 2006
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.

## 2 Systèmes affectés

- VMware ESX Server 2.5.4 Upgrade Patch 1 ;
- VMware ESX Server 2.1.3 Upgrade Patch 2 ;
- VMware ESX Server 2.0.2 Upgrade Patch 2 ;
- VMware ESX Server 3.0.0 AMD fxsave/restore issue.

## 3 Description

De multiples vulnérabilités ont été découvertes dans le produit VMware ESX Server. Ces vulnérabilités permettent à un utilisateur mal intentionné de provoquer un déni de service à distance et/ou d'exécuter du code arbitraire à distance.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Bulletins de sécurité VMware ESX Server :  
<http://www.vmware.com/download/esx/esx-254-200610-patch.html>  
<http://www.vmware.com/download/esx/esx-213-200610-patch.html>  
<http://www.vmware.com/download/esx/esx-202-200610-patch.html>  
<http://kb.vmware.com/kb/2533126>
- Bulletin de sécurité SuSE SUSE-SA:2007:012 :  
<http://lists.suse.com/archive/suse-security-announce/2007-May/0008.html>
- Référence CVE CAN-2004-2069 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-2069>
- Référence CVE CVE-2006-3403 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3403>
- Référence CVE CVE-2005-2177 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2177>
- Référence CVE CVE-2006-3467 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3467>
- Référence CVE CVE-2006-1056 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1056>
- Référence CVE CVE-2006-1342 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1342>
- Référence CVE CVE-2006-1343 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1343>
- Référence CVE CVE-2006-1864 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1864>
- Référence CVE CVE-2006-2071 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2071>

## Gestion détaillée du document

**15 novembre 2006** version initiale.

**29 mai 2007** ajout de la référence au bulletin de sécurité SuSE.