

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans VMware ESX et ESXi

---

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-271>

---

### Gestion du document

Référence	CERTA-2011-AVI-271
Titre	Vulnérabilités dans VMware ESX et ESXi
Date de la première version	29 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware WMSA-2011-0007 du 28 avril 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

- Dénis de service à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMware ESX 4.0 et 4.1 ;
- VMware ESXi 4.0 et 4.1.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans VMware ESX et ESXi permettant à un utilisateur malintentionné de provoquer un déni de service, une élévation de privilèges ou un contournement de la politique de sécurité.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans les produits VMware ESX et ESXi :

- Une vulnérabilité (CVE-2010-2240) présente dans le noyau Linux (cf. avi CERTA CERTA-2010-AVI-392) ;
- quatre vulnérabilités (CVE-2010-1323, CVE-2010-1324, CVE-2010-4020 et CVE-2010-4021) présentes dans Kerberos (cf. avi CERTA CERTA-2010-AVI-571) ;
- deux vulnérabilités (CVE-2011-1785 et CVE-2011-1786) concernent la gestion des ressources réseau.

## 5 Solution

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

## 6 Documentation

- Document du CERTA CERTA-2010-AVI-392 du 19 août 2010 (CVE-2010-2240) :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-392/index.html>
- Document du CERTA CERTA-2010-AVI-571 du 01 décembre 2010 (CVE-2010-1323, CVE-2010-1324, CVE-2010-4020 et CVE-2010-4021) :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-571/index.html>
- Bulletin de sécurité VMware VMSA-2011-0007 du 28 avril 2011 :  
<http://www.vmware.com/security/advisories/VMSA-2011-0007.html>
- Référence CVE CVE-2010-2240 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2240>
- Référence CVE CVE-2010-1323 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1323>
- Référence CVE CVE-2010-1324 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1324>
- Référence CVE CVE-2010-4020 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4020>
- Référence CVE CVE-2010-4021 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4021>
- Référence CVE CVE-2011-1785 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1785>
- Référence CVE CVE-2011-1786 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1786>

## Gestion détaillée du document

29 avril 2011 version initiale.