

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-2011-AVI-423>

---

### Gestion du document

Référence	CERTA-2011-AVI-423
Titre	Multiples vulnérabilités dans VMware ESX
Date de la première version	01 août 2011
Date de la dernière version	–
Source(s)	Avis de sécurité VMware VMSA-2011-0010 du 28 juillet 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 ;
- élévation de privilèges.

## 2 Systèmes affectés

- VMware ESX 3.0.x ;
- VMware ESX 3.5.x ;
- VMware ESX 4.0.x ;
- VMware ESX 4.1.x.

## 3 Résumé

De multiples vulnérabilités affectant différents logiciels inclus dans VMware ESX Console OS (COS) ont été corrigées.

## 4 Description

Plusieurs logiciels vulnérables inclus dans VMware ESX Console OS ont été mis à jour par l'éditeur :

- DHCP est mis à jour pour corriger une vulnérabilité permettant à un utilisateur malveillant distant de provoquer un déni de service et d'exécuter du code arbitraire (CVE-2011-0997) ;
- `glIBC` est mise à jour pour corriger de multiples vulnérabilités exploitables localement (CVE 2010-0296, CVE-2011-0536, CVE-2011-997 et CVE-2011-1071).

## 5 Solution

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

VMware fournit pour l'instant des correctifs pour la version 4.1 d'ESX. Les correctifs pour les versions 4.0 et 3.5 ont été annoncés.

## 6 Documentation

- Bulletin de sécurité VMware VMSA-2011-0010 du 28 juillet 2011 :  
<http://www.vmware.com/security/advisories/VMSA-2011-0010.html>
- Référence CVE CVE-2010-0296 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0296>
- Référence CVE CVE-2011-0536 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0536>
- Référence CVE CVE-2011-0997 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0997>
- Référence CVE CVE-2011-1071 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1071>
- Référence CVE CVE-2011-1095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1095>
- Avis CERTA CERTA-2011-AVI-190 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-190/>
- Avis CERTA CERTA-2011-AVI-193 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-193/>

## Gestion détaillée du document

01 août 2011 version initiale.