

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de VMware ESX Server

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-2007-AVI-154>

Gestion du document

Référence	CERTA-2007-AVI-154
Titre	Multiples vulnérabilités de VMware ESX Server
Date de la première version	03 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de mise à jour de VMware
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 ;
- élévation de privilèges.

2 Systèmes affectés

- VMware ESX Server 2.x ;
- VMware ESX Server 3.x.

3 Description

De multiples vulnérabilités ont été découvertes dans VMware ESX Server. Ces vulnérabilités peuvent être exploitées par un utilisateur malintentionné afin de conduire des dénis de service, de contourner la politique de sécurité mise en place, ou d'exécuter du code arbitraire à distance afin de prendre le contrôle total de la machine hébergeant le service vulnérable.

4 Solution

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

5 Documentation

- Site de l'éditeur :
<http://www.vmware.com>
- Bulletin de mise à jour de l'éditeur du 30 mars 2007:
<http://kb.vmware.com/kb/5031800>
<http://kb.vmware.com/kb/5885387>
<http://kb.vmware.com/kb/6856573>
<http://kb.vmware.com/kb/3003211>
<http://kb.vmware.com/kb/3194055>
<http://kb.vmware.com/kb/3496682>
- Référence CVE CVE-2006-3739 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3739>
- Référence CVE CVE-2006-3740 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3740>
- Référence CVE CVE-2006-4334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4334>
- Référence CVE CVE-2006-4335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4335>
- Référence CVE CVE-2006-4336 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4336>
- Référence CVE CVE-2006-4337 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4337>
- Référence CVE CVE-2006-4338 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4338>
- Référence CVE CVE-2006-6097 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6097>

Gestion détaillée du document

03 avril 2007 version initiale.