

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2008-AVI-116>

Gestion du document

Référence	CERTA-2008-AVI-116
Titre	Vulnérabilité de VMware ESX Server
Date de la première version	06 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-0004
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 ;
- déni de service.

2 Systèmes affectés

VMware ESX Server 2.x.

3 Résumé

Une vulnérabilité dans VMware ESX Server permet à un utilisateur de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

VMware ESX Server est un serveur de machines virtuelles. Celui-ci s'appuie sur un certain nombre de logiciels libres pour mettre en œuvre certaines de ses fonctionnalités. En particulier, il embarque le logiciel `e2fsprogs` permettant la manipulation de systèmes de fichiers `ext2`. Or, la version de `e2fsprogs` utilisée

par `ESX Server` comporte plusieurs failles permettant à un utilisateur de provoquer un déni de service ou d'exécuter du code arbitraire via un fichier contenant un système de fichiers `ext2` construit de façon particulière.

5 Solution

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

6 Documentation

- Site de VMware :
<http://www.vmware.com>
- Bulletin de sécurité VMware VMSA-2008-0004 du 03 mars 2008 :
<http://lists.vmware.com/pipermail/security-announce/2008/000007.html>
- Référence CVE CVE-2007-5497 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5497>

Gestion détaillée du document

06 mars 2008 version initiale.