

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-2008-AVI-283>

Gestion du document

Référence	CERTA-2008-AVI-283
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	04 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-0008 du 30 mai 2008
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.

2 Systèmes affectés

- VMware Workstation 6.0.3 et versions antérieures ;
- VMware Player 2.0.3 et versions antérieures ;
- VMware ACE 2.0.3 et versions antérieures ;
- VMware Fusion 1.1.1 et versions antérieures.

3 Résumé

Deux vulnérabilités affectent les produits VMware. Elles permettent à une personne malveillante ayant accès au système virtualisé d'exécuter du code arbitraire sur l'hôte.

4 Description

La première vulnérabilité affecte la fonctionnalité HGFS (*Host Guest File System*) qui permet de réaliser un partage de fichiers entre le système virtualisé et le système hôte. Une vulnérabilité de type débordement de mémoire permet à une personne malveillant d'exécuter du code arbitraire sur le système réel.

Cette vulnérabilité n'est pas exploitable dans la configuratin par défaut, sachant qu'aucun répertoire n'est partagé.

La seconde vulnérabilité affecte le service VMCI (*Virtual Machine Communication Interface*). Cette vulnérabilité permet à une personne malveillante d'exécuter du code arbitraire sur le système hôte fonctionnant sous Microsoft Windows. Cette vulnérabilité est causée par une erreur dans le traitement des fichiers de configuration vmx.

5 Solution

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

6 Documentation

- Bulletin de sécurité VMware VMSA-2008-0008 du 30 mai 2008 :
<http://www.vmware.com/security/advisories/VMSA-2008-0008.html>
- Référence CVE CVE-2008-2098 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2098>
- Référence CVE CVE-2008-2099 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2099>

Gestion détaillée du document

04 juin 2008 version initiale.