

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du logiciel VMware Fusion

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-2009-AVI-419>

Gestion du document

Référence	CERTA-2009-AVI-419
Titre	Multiples vulnérabilités du logiciel VMware Fusion
Date de la première version	02 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware numéro VMSA-2009-0013 du 01 octobre 2009
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

- Déni de service ;
- exécution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

VMware Fusion version 2.0.5 et versions antérieures

3 Résumé

De multiples vulnérabilité permettant de provoquer un déni de service ou d'obtenir des privilèges plus élevés ont été découvertes dans VMware Fusion.

4 Description

Deux vulnérabilités ont été découvertes dans VMware Fusion :

- la première vulnérabilité est due à une erreur au niveau de l'extension noyau *vmx86*. L'exploitation de cette vulnérabilité permet d'exécuter du code arbitraire dans le contexte du noyau du système hôte ;

- la seconde vulnérabilité résulte d'un dépassement de capacité d'entier au niveau de l'extension noyau *vmx86*. Cette vulnérabilité peut être exploitée par un utilisateur malintentionné afin de causer un déni de service.

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 numéro VMSA-2009-0013 du 01 octobre 2009 :
<http://lists.vmware.com/pipermail/security-announce/2009/000066.html>
- Référence CVE CVE-2009-3281 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3281>
- Référence CVE CVE-2009-3282 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3282>

Gestion détaillée du document

02 octobre 2009 version initiale.