



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 18 septembre 2009
N° CERTA-2009-AVI-389

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2009-AVI-389>

Gestion du document

Référence	CERTA-2009-AVI-389
Titre	Multiples vulnérabilités dans VMware
Date de la première version	18 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de mise à jour VMware VMSA-2009-0012
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.

2 Systèmes affectés

- VMware Workstation Movie Decoder version 6.5.2 et version antérieures ;
- VMware Workstation version 6.5.2 et versions antérieures ;
- VMware Player version 2.5.2 et versions antérieures ;
- VMware ACE version 2.5.2 et versions antérieures.

3 Résumé

De multiples vulnérabilités permettant d'exécuter du code arbitraire à distance ont été découvertes dans les produits VMware.

4 Description

De multiples vulnérabilités ont été découvertes dans la gestion de certains formats vidéo via la bibliothèque `vmnc.dll` des produits VMware. L'exploitation de ces vulnérabilités permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance via un fichier vidéo spécialement construit.

5 Solution

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

6 Documentation

- Bulletin de mise à jour VMware VMSA-2009-0012 :
<http://lists.vmware.com/pipermail/security-announce/2009/000065.html>
- Référence CVE CVE-2009-0199 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0199>
- Référence CVE CVE-2009-0910 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0910>
- Référence CVE CVE-2009-2628 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2628>

Gestion détaillée du document

18 septembre 2009 version initiale.