Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 décembre 2010
N° CERTA-2010-AVI-574

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits VMware

Gestion du document

Référence	CERTA-2010-AVI-574
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	03 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0018 du 02 décembre 2010
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 ;
- exécution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

- VMware Workstation version 7.1.1 et antérieures ;
- VMware Workstation version 6.5.4 et antérieures ;
- VMware Player version 3.1.1 et antérieures ;
- VMware Player version 2.5.4 et antérieures ;
- VMware Fusion version 3.1.1 et antérieures ;
- VMware ESXi 4.1 sans le correctif ESXi410-201010402-BG ou postérieurs ;
- VMware ESXi 4.0 sans le correctif ESXi400-201009402-BG ou postérieurs ;
- VMware ESXi 3.5 sans le correctif ESXi350-201008402-BG ou postérieurs ;
- VMware ESX 4.1 sans le correctif ESX410-201010405-BG ;
- VMware ESX 4.0 sans le correctif ESX400-201009401-BG ;
- VMware ESX 3.5 sans le correctif ESX350-201008409-BG ;

3 Résumé

Plusieurs vulnérabilités dans les produits `VMware` permettent à une personne malintentionnée d'exécuter du code arbitraire en local ou à distance ou d'élever ses privilèges sur le système vulnérable.

4 Description

Plusieurs vulnérabilités dans les produits `VMware` ont été découvertes :

- une vulnérabilité dans le codec *VMnc* permet à une personne malintentionnée d'exécuter du code arbitraire à distance (CVE-2010-4294) ;
- une vulnérabilité dans la gestion des fichiers temporaires par le processus de montage permet à une personne malintentionnée d'élever ses privilèges sur le système hôte (CVE-2010-4295) ;
- une vulnérabilité dans le fichier binaire *vmware-mount* permet à une personne malintentionnée d'exécuter du code sur la machine hôte avec les privilèges de l'utilisateur « *root* » (CVE-2010-4296) ;
- une vulnérabilité dans la validation des données d'entrée de la mise à jour de `VMware Tools` permet à une personne malintentionnée d'exécuter du code arbitraire avec les privilèges de l'utilisateur « *root* » sur la machine invitée (CVE-2010-4297).

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-2010-0018 du 02 décembre 2010 :
  http://www.vmware.com/security/advisories/VMSA-2010-0018.html
- Référence CVE CVE-2010-4294 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4294
- Référence CVE CVE-2010-4295 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4295
- Référence CVE CVE-2010-4296 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4296
- Référence CVE CVE-2010-4297 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4297

Gestion détaillée du document

03 décembre 2010 version initiale.