Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2012
N° CERTA-2012-AVI-249

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware

Gestion du document

Référence	CERTA-2012-AVI-249
Titre	Multiples vulnérabilités dans VMware
Date de la première version	04 mai 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2012-0009 du 03 mai 2012
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 ;
- élévation de privilèges.

2 Systèmes affectés

- ESXi 5.0 ;
- ESXi 4.1 ;
- ESXi 4.0 ;
- ESXi 3.5 ;
- ESX 4.1 ;
- ESX 4.0 ;
- ESX 3.5 ;
- versions antérieures à Workstation 8.0.3 ;
- versions antérieures à Player 4.0.3 ;
- versions antérieures à Fusion 4.1.2.

3 Résumé

Cinq vulnérabilités ont été corrigées dans les produits *VMware*. Deux concernent les commandes RPC, il est possible de manipuler un pointeur dans le processus VMX, grâce ce pointeur un utilisateur peut exécuter du code arbitraire depuis l'environnement virtuel sur l'hôte. La troisième concerne les échanges NFS sur le réseau et peut elle aussi mener à une exécution de code arbitraire sur l'hôte ESX/ESXi sans authentification. La quatrième permet d'écrire en dehors de l'espace mémoire virtuelle au moyen du lecteur de disquette virtualisé. Enfin, il est possible d'écrire de façon arbitraire en mémoire au moyen d'un lecteur virtuel SCSI, il est ainsi possible d'exécuter du code depuis une machine virtuelle vers l'hôte.

4 Solution

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

5 Documentation

- Bulletin de sécurité VMware VMSA-2012-0009 du 03 mai 2012 :
  http://www.vmware.com/security/advisories/VMSA-2012-0009.html
- Référence CVE CVE-2012-1516 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1516
- Référence CVE CVE-2012-1517 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1517
- Référence CVE CVE-2012-2448 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2448
- Référence CVE CVE-2012-2449 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2449
- Référence CVE CVE-2012-2450 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2450

Gestion détaillée du document

04 mai 2012 version initiale.