Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 janvier 2007
N° CERTA-2007-AVI-026

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware

Gestion du document

Référence	CERTA-2007-AVI-026
Titre	Multiples vulnérabilités dans VMware
Date de la première version	11 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2007-0001 du 09 janvier 2007
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 ;
- déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- VMware ESX Server 3.0.x ;
- VMware ESX Server 2.x.

3 Résumé

De multiples vulnérabilités ont été corrigées pour les produits VMware ESX Server 2.x et 3.0.x.

4 Description

De multiples vulnérabilités ont été découvertes dans le produit VMware ESX Server. Celles-ci concernent :

- Une mauvaise gestion des droits sur les clés SSL générées par `vmware-config` (CVE-2006-3589) ;
- certaines bibilothèques OpenSSL (CVE-2006-2937, CVE-2006-2940, CVE-2006-4339, CVE-2006-4343, CVE-2006-3738) ;
- OpenSSH (CVE-2004-2069, CVE-2006-0225, CVE-2003-0386, CVE-2006-4924, CVE-2006-5051, CVE-2006-5794) ;
- un débordement de tampon dans la fonction repr() utilisée par certaines applications en Python (CVE-2006-4980) ;
- un problème concernant les fichiers de disques virtuels (`.vmdk` ou `.dsk`) nouvellement créés, qui contiennent des blocs de fichiers de disques récemment effacés.

5 Solution

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

6 Documentation

- Patch pour VMware ESX Server 2.0.2 :
  http://www.vmware.com/support/esx2/doc/esx-202-200612-patch.html
- Patch pour VMWare ESX Server 2.1.3 :
  http://www.vmware.com/support/esx21/doc/esx-213-200612-patch.html
- Patch pour VMWare ESX Server 2.5.3 :
  http://www.vmware.com/support/esx25/doc/esx-253-200612-patch.html
- Patch pour VMware ESX Server 2.5.4 :
  http://www.vmware.com/support/esx25/doc/esx-254-200612-patch.html
- Patch pour VMware ESX Server 3.0.0 :
  http://www.vmware.com/support/vi3/doc/esx-3069097-patch.html
- Patch pour VMware ESX Server 3.0.1 :
  http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
- Référence CVE CVE-2006-3589 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3589
- Référence CVE CVE-2006-2937 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
- Référence CVE CVE-2006-2940 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
- Référence CVE CVE-2006-3738 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
- Référence CVE CVE-2006-4339 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339
- Référence CVE CVE-2006-4343 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343
- Référence CVE CVE-2004-2069 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2069
- Référence CVE CVE-2003-0386 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0386
- Référence CVE CVE-2006-4924 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4924
- Référence CVE CVE-2006-4980 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4980
- Référence CVE CVE-2006-0225 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0225

- Référence CVE CVE-2006-5051 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5051
- Référence CVE CVE-2006-5794 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5794

Gestion détaillée du document

11 janvier 2007 version initiale.