Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 novembre 2007
N° CERTA-2007-AVI-409-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits VMware

Gestion du document

Référence	CERTA-2007-AVI-409-001
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	21 septembre 2007
Date de la dernière version	20 novembre 2007
Source(s)	Avis de sécurité VMware VMSA-2007-0006 du 18 septembre 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 ;
- déni de service ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- VMware Workstation 6.0.0 ;
- VMware Workstation 5.5.4 ainsi que les versions antérieures ;
- VMware Player version 2.0.0 ;
- VMware Player 1.0.4 ainsi que les versions antérieures ;
- VMware Server 1.0.3 ainsi que les versions antérieures ;
- VMware ACE 2.0.0 ;
- VMware ACE 1.0.3 ainsi que les versions antérieures ;
- VMware ESX, pour les versions 3.0.0, 3.0.1 et 3.0.2 sans les patchs associés ;
- VMware ESX 2.5.4 sans le patch 10 ;
- VMware ESX 2.5.3 sans le patch 13 ;
- VMware ESX 2.1.3 sans le patch 8 ;
- VMware ESX 2.0.2 sans le patch 8 ;

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans différents produits VMware. L'exploitation de ces derniers peut provoquer l'exécution de code arbitraire depuis une machine virtuelle sur la machine hôte, ou perturber son fonctionnement.

4 Description

Plusieurs vulnérabilités ont été identifiées dans différents produits VMware. Parmi celles-ci :

- un utilisateur ayant des droits administrateur sur la machine virtuelle peut parvenir à corrompre la mémoire du processus hôte, et donc potentiellement exécuter du code arbitraire sur le système d'accueil ;
- un erreur de manipulation dans le serveur DHCP peut être exploitée au moins de paquets spécialement construits pour acquérir les droits administrateur sur le système hôte vulnérable ;
- plusieurs problèmes dans la manipulation de requêtes MS-RPC de SAMBA peuvent être exploités pour provoquer un débordement de pile côté serveur.
- une vulnérabilité du serveur DNS, associée à l'avis CERTA-2007-AVI-327 concernant BIND ;
- etc.

5 Solution

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

6 Documentation

- Site officiel de Vmware :
  http://www.vmware.com/security
- Liste de diffusion des annonces de sécurité VMware :
  http://lists.vmware.com/cgi-bin/mailman/listinfo/security-announce
- Copie de l'annonce de sécurité VMSA-2007-0006 de VMware publiée le 18 septembre 2007 :
  http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065902.html
- Bulletin de sécurité Gentoo GLSA 200711-23 du 18 novembre 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200711-23.xml
- Référence CVE CVE-2004-0813 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0813
- Référence CVE CVE-2006-1174 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1174
- Référence CVE CVE-2006-3619 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3619
- Référence CVE CVE-2006-4146 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4146
- Référence CVE CVE-2006-4600 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4600
- Référence CVE CVE-2007-0061 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0061
- Référence CVE CVE-2007-0062 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0062
- Référence CVE CVE-2007-0063 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0063
- Référence CVE CVE-2007-0494 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0494
- Référence CVE CVE-2007-1716 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1716

- Référence CVE CVE-2007-1856 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1856
- Référence CVE CVE-2007-2442 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2442
- Référence CVE CVE-2007-2443 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2443
- Référence CVE CVE-2007-2446 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2446
- Référence CVE CVE-2007-2447 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447
- Référence CVE CVE-2007-2798 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2798
- Référence CVE CVE-2007-4496 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4496
- Référence CVE CVE-2007-4497 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4497

Gestion détaillée du document

21 septembre 2007 version initiale.
20 novembre 2007 Ajout de la référence au bulletin de sécurité Gentoo.