Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2008
N° CERTA-2008-AVI-380

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware ESX

Gestion du document

Référence	CERTA-2008-AVI-380
Titre	Multiples vulnérabilités dans VMware ESX
Date de la première version	29 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-00011 du 28 juillet 2008
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

VMware ESX 3.5, sans les correctifs ESX350-200806201-UG et ESX350-200806218-UG, ainsi que les versions antérieures, sont vulnérables.

3 Résumé

Plusieurs vulnérabilités affectant les services `Samba` et `vmnix` de `VMware ESX` ont été corrigées.

4 Description

Plusieurs vulnérabilités permettant, entre autres, de provoquer des dénis de service et d'exécuter du code arbitraire à distance ont été corrigées. Elles concernent les services de partage de fichier `Samba` et de console `vmnix`.

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-2008-00011 du 28 juillet 2008 :
  http://lists.vmware.com/pipermail/security-announce/2008/000023.html
- Référence CVE CVE-2006-4814 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4814
- Référence CVE CVE-2007-5001 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5001
- Référence CVE CVE-2007-6151 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6151
- Référence CVE CVE-2007-6206 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6206
- Référence CVE CVE-2008-0007 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0007
- Référence CVE CVE-2008-1105 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1105
- Référence CVE CVE-2008-1367 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1367
- Référence CVE CVE-2008-1375 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1375
- Référence CVE CVE-2008-1669 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1669

Gestion détaillée du document

29 juillet 2008 version initiale.