



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 mars 2008
N° CERTA-2008-AVI-141

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les produits VMware

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-141>

Gestion du document

Référence	CERTA-2008-AVI-141
Titre	Vulnérabilités dans les produits VMware
Date de la première version	18 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-005 du 17 mars 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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- VMware Workstation 6.0.x ;
- VMware Workstation 5.5.x ;
- VMware Player 2.0.x ;
- VMware Player 1.0.x ;
- VMware ACE 2.0.x ;
- VMware ACE 1.0.x ;
- VMware Server 1.0.x ;
- VMware Fusion 1.x.

3 Description

Plusieurs vulnérabilités découvertes dans les produits `VMware` permettent à un utilisateur malveillant, à partir d'un système virtualisé, de contourner la politique de sécurité pour porter atteinte à la confidentialité et à l'intégrité des données du système hôte.

D'autres vulnérabilités permettent à un utilisateur malintentionné de provoquer un déni de service ou d'élever ses privilèges à l'intérieur d'un système virtuel.

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-2008-0005 du 17 mars 2008 :
<http://www.vmware.com/security/advisories/VMSA-2008-0005.shtml>
- 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-2006-4339 :
<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-2007-5269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5269>
- Référence CVE CVE-2007-5618 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5618>
- Référence CVE CVE-2008-1340 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1340>
- Référence CVE CVE-2008-1361 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1361>
- Référence CVE CVE-2008-1362 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1362>
- Référence CVE CVE-2008-1363 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1363>
- Référence CVE CVE-2008-1364 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1364>

Gestion détaillée du document

18 mars 2008 version initiale.