

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware ESX Server

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-2010-AVI-293>

Gestion du document

Référence	CERTA-2010-AVI-293
Titre	Multiples vulnérabilités dans VMware ESX Server
Date de la première version	28 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware #1022899 du 24 juin 2010
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

VMware ESX 3.5 sans le correctif ESX350-201006401-SG.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans VMware ESX. Elles permettent, entre autre, l'élévation de privilèges.

4 Description

Plusieurs vulnérabilités ont été corrigées dans VMware ESX dont certaines liées à la mise à jour du noyau linux kernel-2.4.21-60.

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 #1022899 du 24 juin 2010 :
<http://kb.vmware.com/kb/1022899>
- Référence CVE CVE-2008-5029 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5029>
- Référence CVE CVE-2008-5300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5300>
- Référence CVE CVE-2009-1337 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1337>
- Référence CVE CVE-2009-1385 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1385>
- Référence CVE CVE-2009-1895 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1895>
- Référence CVE CVE-2009-2848 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2848>
- Référence CVE CVE-2009-3002 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3002>
- Référence CVE CVE-2009-3547 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3547>
- Référence CVE CVE-2009-2698 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2698>
- Référence CVE CVE-2009-2692 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692>

Gestion détaillée du document

28 juin 2010 version initiale.