

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans des 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-483>

Gestion du document

Référence	CERTA-2008-AVI-483
Titre	Multiples vulnérabilités dans des produits VMware
Date de la première version	06 octobre 2008
Date de la dernière version	–
Source(s)	Avis de sécurité VMware VMSA-2008-0016 du 03 octobre 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- VMware VirtualCenter 2.5 pour les versions antérieures à Update 3 build 119838 ;
- VMware Workstation pour la version 6.0.4 ainsi que celles antérieures ;
- VMware Workstation pour la version 5.5.7 ainsi que celles antérieures ;
- VMware Player pour la version 2.0.4 ainsi que celles antérieures ;
- VMware Player pour la version 1.0.7 ainsi que celles antérieures ;
- VMware ACE pour la version 2.0.4 ainsi que celles antérieures ;
- VMware ACE pour la version 1.0.6 ainsi que celles antérieures ;
- VMware Server pour la version 1.0.6 ainsi que celles antérieures ;
- VMware ESXi 3.5 sans le correctif ESXe350-200809401-I-SG ;
- VMware ESX 3.5 sans le correctif ESX350-200809404-SG ;
- VMware ESX 3.0.3 sans le correctif ESX303-200809401-SG ;

- VMware ESX 3.0.2 sans le correctif ESX-1006361 ;
- VMware ESX 3.0.1 sans le correctif ESX-1006678.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les systèmes de virtualisation VMware. L'exploitation de ces dernières peut conduire à une élévation de privilèges à partir d'un système invité (64-bit) ou à l'apparition en clair du mot de passe de l'utilisateur se connectant à VirtualCenter. D'autres vulnérabilités permettent de contourner la politique de sécurité mise en place.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les systèmes de virtualisation VMware :

- le mot de passe utilisateur peut apparaître en clair au cours de la connexion au serveur VirtualCenter ;
- plusieurs vulnérabilités Sun Java JDK / JRE peuvent être exploitées pour perturber le fonctionnement du système ou contourner certaines restrictions de sécurité ;
- certaines instructions x64 ne sont pas émulées correctement. Cette vulnérabilité peut être exploitée par un utilisateur sur un système « invité » pour élever ses privilèges (cf. l'avis CERTA-2008-AVI-445).

5 Solution

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

6 Documentation

- Bulletin de sécurité VMware VMSA-2008-0016 du 03 octobre 2008 :
<http://www.vmware.com/security/advisories/VMSA-2008-0016.html>
- Référence CVE CVE-2008-3103 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3103>
- Référence CVE CVE-2008-3104 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3104>
- Référence CVE CVE-2008-3105 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3105>
- Référence CVE CVE-2008-3106 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3106>
- Référence CVE CVE-2008-3107 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3107>
- Référence CVE CVE-2008-3108 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3108>
- Référence CVE CVE-2008-3109 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3109>
- Référence CVE CVE-2008-3110 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3110>
- Référence CVE CVE-2008-3111 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3111>
- Référence CVE CVE-2008-3112 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3112>
- Référence CVE CVE-2008-3113 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3113>
- Référence CVE CVE-2008-3114 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3114>
- Référence CVE CVE-2008-3115 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3115>

- Référence CVE CVE-2008-4278 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4278>
- Référence CVE CVE-2008-4279 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4279>

Gestion détaillée du document

06 octobre 2008 version initiale.