



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2010
N° CERTA-2010-AVI-141

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2010-AVI-141>

Gestion du document

Référence	CERTA-2010-AVI-141
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	30 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-005 du 29 mars 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

Injection de code indirecte.

2 Systèmes affectés

- Virtual Center 2.5 ;
- Virtual Center 2.0.2 ;
- VMware Server 2.0.2 ;
- VMware Server 1.0.10 ;
- ESX 3.5 ;
- ESX 3.0.3.

3 Résumé

Plusieurs vulnérabilités dans les produits VMware avec *WebAccess* permettent à une personne malintentionnée d'effectuer des injections de code indirectes.

4 Description

De multiples faiblesses dans le contrôle de certains paramètres dans les produits VMware avec *WebAccess* permettent à une personne malintentionnée d'effectuer des injections de code indirectes.

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-2010-0005 du 29 mars 2010 :
<http://www.vmware.com/security/advisories/VMSA-2010-0005.html/>
- Référence CVE CVE-2009-2277 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2277>
- Référence CVE CVE-2010-0686 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0686>
- Référence CVE CVE-2010-1137 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1137>
- Référence CVE CVE-2010-1193 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1193>

Gestion détaillée du document

30 mars 2010 version initiale.