



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2010
N° CERTA-2010-AVI-306

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware Studio

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-306>

Gestion du document

Référence	CERTA-2010-AVI-306
Titre	Multiples vulnérabilités dans VMware Studio
Date de la première version	13 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0011 du 13 juillet 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

- Exécution de code arbitraire à distance ;
- élévation de privilèges.

2 Systèmes affectés

- VMware Studio 2.0 ;
- Machines virtuelles créées avec VMware Studio 2.0.

3 Résumé

De multiples vulnérabilités dans VMware Studio 2.0, ainsi que les machines virtuelles créées avec celui-ci, permettent, entre autres, l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été identifiées dans VMware Studio 2.0. Leur exploitation permet à une personne malintentionnée d'exécuter du code arbitraire à distance, ou d'élever ses privilèges.

Les machines virtuelles créées avec VMware Studio 2.0 sont elles aussi vulnérables. Pour corriger les machines virtuelles concernées, il est nécessaire de les recréer avec une version non vulnérable de VMware Studio (version 2.1).

5 Solution

La version 2.1 de VMware Studio 2.0 corrige ces problèmes.

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

6 Documentation

- Bulletin de sécurité VMware VMSA-2010-0011 du 13 juillet 2010 :
<http://www.vmware.com/security/advisories/VMSA-2010-0011.html>
- Référence CVE CVE-2010-2427 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2427>
- Référence CVE CVE-2010-2667 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2667>

Gestion détaillée du document

13 juillet 2010 version initiale.