Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juillet 2010
N° CERTA-2010-AVI-326

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans VMware vCenter Update Manager

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-326`

Gestion du document

Référence	CERTA-2010-AVI-326
Titre	Vulnérabilités dans VMware vCenter Update Manager
Date de la première version	20 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0012 du 19 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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- VMware vCenter Update Manager 1.0 ;
- VMware vCenter Update Manager 4.0 ;
- VMware vCenter Update Manager 4.1.

3 Résumé

Deux vulnérabilités dans `VMware vCenter Update Manager` permettent d'effectuer une injection de code indirecte ou de porter atteinte à la confidentialité des données.

4 Description

Deux vulnérabilités ont été découvertes dans `VMware vCenter Update Manager`:

- une vulnérabilité de type « *directory traversal* » permet de porter atteinte à la confidentialité des données (CVE-2009-1523) ;
- une injection de code indirecte dans `Jetty` autorise l'exécution de *JavaScript* si un utilisateur clique sur un lien malveillant (CVE-2009-1524).

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva VMSA-2010-0012 du 19 juillet 2010 :
  http://www.vmware.com/security/advisories/VMSA-2010-0012.html
- Référence CVE CVE-2009-1523 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1523
- Référence CVE CVE-2009-1524 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1524

Gestion détaillée du document

20 juillet 2010 version initiale.