Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2010
N° CERTA-2010-AVI-553

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware ESX et ESXi

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-553

Gestion du document

Référence	CERTA-2010-AVI-553
Titre	Multiples vulnérabilités dans VMWare ESX et ESXi
Date de la première version	17 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2010-0016 du 15 novembre 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 ;
- déni de service à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- VMware ESX versions 4.0 et 4.1 ;
- VMware ESXi version 4.1.

3 Résumé

De multiples vulnérabilités sont présentes dans *VMware ESX* et *ESXi*. L'exploitation réussie de celles-ci permet entre autres l'exécution de code arbitraire à distance.

4 Description

Une mise à jour du noyau de `Service Console OS` corrige les vulnérabilités suivantes:

- CVE-2010-0291 (élévation de privilèges et déni de service)
- CVE-2010-0307 (déni de service)
- CVE-2010-0415 (déni de service)
- CVE-2010-0622 (déni de service)
- CVE-2010-1087 (déni de service)
- CVE-2010-1088 (impact non défini)
- CVE-2010-1437 (déni de service)

La version 4.0 de *VMware ESX* est impactée mais le correctif n'est pas encore disponible à la date de rédaction de cet avis.

De même une mise à jour des paquets *likewise* corrige les vulnérabilités suivantes:

- CVE-2009-0844 (déni de service à distance)
- CVE-2009-0845 (déni de service à distance)
- CVE-2009-0846 (exécution de code arbitraire à distance)
- CVE-2009-4212 (exécution de code arbitraire à distance)
- CVE-2010-1321 (déni de service)

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-2010-0016 du 15 novembre 2010
  http://lists.vmware.com/pipermail/security-announce/2010/000108.html
- Référence CVE CVE-2010-0291 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0291
- Référence CVE CVE-2010-0307 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0307
- Référence CVE CVE-2010-0415 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0415
- Référence CVE CVE-2010-0622 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0622
- Référence CVE CVE-2010-1087 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1087
- Référence CVE CVE-2010-1088 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1088
- Référence CVE CVE-2010-1437 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1437
- Référence CVE CVE-2009-0844 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0844
- Référence CVE CVE-2009-0845 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0845
- Référence CVE CVE-2009-0846 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0846
- Référence CVE CVE-2009-4212 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4212
- Référence CVE CVE-2010-1321 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1321

Gestion détaillée du document

17 novembre 2010 version initiale.