

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware ESX Server

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-461>

Gestion du document

Référence	CERTA-2010-AVI-461
Titre	Multiples vulnérabilités dans VMware ESX Server
Date de la première version	01 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMSA-2010-0015 du 30 septembre 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

- Dénis de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

VMware ESX 4.0 Console OS (COS).

3 Résumé

De nombreuses vulnérabilités affectant différents logiciels inclus dans *VMware ESX Console OS* ont été corrigées.

4 Description

Plusieurs logiciels vulnérables inclus dans *VMware ESX Console OS* ont été mis à jour par l'éditeur :

- le composant *NSS_db* est mis à jour pour corriger une vulnérabilité permettant à un utilisateur malveillant d'accéder à des données confidentielles (CVE-2010-0826) ;
- une mise à jour du composant *OpenLDAP* corrige un erreur dans la gestion du Common Name d'un certificat X.509, qui permet une attaque du type « homme au milieu » (CVE-2009-3767) ;
- la bibliothèque *libcurl* est mise à jour afin de corriger une vulnérabilité permettant à un attaquant d'effectuer à distance un déni de service par arrêt inopiné (CVE-2010-0734) ;
- le logiciel *sudo* est mis à jour pour corriger une erreur concernant la gestion d'une variable d'environnement permettant à un utilisateur malveillant d'élever ses privilèges (CVE-2010-1646) ;
- une mise à jour groupée des composants *OpenSSL*, *GnuTLS*, *NSS* et *NSPR* corrige différentes vulnérabilités permettant entre autres un déni de service et l'élévation de privilèges (CVE-2009-3555, CVE-2009-2409, CVE-2009-3245 et CVE-2010-0433).

5 Solution

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

6 Documentation

- Bulletin de sécurité VMSA-2010-0015 du 30 septembre 2010 :
<http://lists.vmware.com/pipermail/security-announce/2010/000106.html>
- Référence CVE CVE-2009-2409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409>
- Référence CVE CVE-2009-3245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3245>
- Référence CVE CVE-2009-3555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
- Référence CVE CVE-2009-3767 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3767>
- Référence CVE CVE-2010-0433 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0433>
- Référence CVE CVE-2010-0734 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0734>
- Référence CVE CVE-2010-0826 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0826>
- Référence CVE CVE-2010-1646 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1646>

Gestion détaillée du document

01 octobre 2010 version initiale.