

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans VMware ESX et ESXi 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-2012-AVI-663>

---

### Gestion du document

Référence	CERTA-2012-AVI-663
Titre	Multiples vulnérabilités dans VMware ESX et ESXi Server
Date de la première version	19 novembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2012-0016 du 15 novembre 2012
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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- VMware ESXi version 4.1 sans le patch ESXi410-201211401-SG
- VMware ESX version 4.1 sans les patches ESX410-201211401-SG, ESX410-201211402-SG, ESX410-201211405-SG et ESX410-201211407-SG

## 3 Résumé

De multiples vulnérabilités ont été corrigées dans *VMware ESX et ESXi Server*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance au moyen d'enregistrements DNS spécialement conçus.

## 4 Solution

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

## 5 Documentation

- Bulletin de sécurité VMware VMSA-2012-0016 du 15 novembre 2012 :  
<http://www.vmware.com/security/advisories/VMSA-2012-0016.html>
- Référence CVE CVE-2011-4940 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4940>
- Référence CVE CVE-2011-4944 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4944>
- Référence CVE CVE-2012-0876 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0876>
- Référence CVE CVE-2012-1033 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1033>
- Référence CVE CVE-2012-1148 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1148>
- Référence CVE CVE-2012-1150 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1150>
- Référence CVE CVE-2012-1667 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1667>
- Référence CVE CVE-2012-2615 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2615>
- Référence CVE CVE-2012-3817 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3817>
- Référence CVE CVE-2012-5703 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5703>

## Gestion détaillée du document

**19 novembre 2012** version initiale.