

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Vulnérabilité dans VMware ESXi**

### Gestion du document

Référence	CERTFR-2016-AVI-425
Titre	Vulnérabilité dans VMware ESXi
Date de la première version	20 décembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2016-0023 du 20 décembre 2016
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(s)

– injection de code indirecte à distance

### 2 - Systèmes affectés

VMware vSphere Hypervisor (ESXi) versions 5.5 et 6.0 sans le dernier correctif de sécurité

### 3 - Résumé

Une vulnérabilité a été corrigée dans *VMware ESXi*. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS).

### 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-2016-0023 du 20 décembre 2016  
<http://www.vmware.com/security/advisories/VMSA-2016-0023.html>

– Référence CVE CVE-2016-7463  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7463>

## **Gestion détaillée du document**

**20 décembre 2016** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-425>

---