



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 septembre 2008  
N° CERTA-2008-AVI-470

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans des produits VMware

---

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-2008-AVI-470>

---

### Gestion du document

Référence	CERTA-2008-AVI-470
Titre	Vulnérabilité dans des produits VMware
Date de la première version	23 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité VMware VMSA-2008-0015 du 18 septembre 2008
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 ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Les versions 3.5 de VMware ESXi et ESX utilisant opensman 2.0.0.

## 3 Résumé

Le service opensman exécuté par VMware EXS et ESXi est vulnérable à deux débordements de mémoire permettant l'exécution de code arbitraire à distance.

## 4 Description

Le service opensman (*Open Web Services Management*) est vulnérable à deux débordements de mémoire lors de la lecture des entêtes des trames HTTP `basic authentication`. Ces vulnérabilités sont exploitables sans identifiants valides et permettent d'exécuter du code arbitraire à distance à l'aide d'une trame spécifiquement conçue.

## **5 Solution**

Se référer au bulletin de sécurité VMware VMSA-2008-0015 du 19 septembre 2008 pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Bulletin de sécurité VMware VMSA-2008-0015 du 19 septembre 2008 :  
<http://www.vmware.com/security/advisories/VMSA-2008-0015.html>
- Référence CVE CVE-2008-2234 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2234>

## **Gestion détaillée du document**

**23 septembre 2008** version initiale.