

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Xen

---

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-061>

---

### Gestion du document

Référence	CERTA-2012-AVI-061-001
Titre	Vulnérabilité dans Xen
Date de la première version	08 février 2012
Date de la dernière version	09 mars 2012
Source(s)	Bulletin de sécurité Debian DSA-2404 du 05 février 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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Xen 4.x.

## 3 Résumé

Une vulnérabilité a été corrigée dans Xen. Elle permet à une machine invitée malveillante de causer un déni de service du système hôte ou d'élérer ses privilèges.

## 4 Description

Une vulnérabilité a été identifiée dans Xen. Elle impacte les systèmes hôtes hébergeant des systèmes invités HVM configurés avec une carte réseau émulée de type e1000. Cette vulnérabilité, de type corruption de mémoire, permet à un système invité malveillant de causer un déni de service du système hôte ou d'élérer ses privilèges.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Debian DSA 2404 du 05 février 2012 :  
<http://www.debian.org/security/2012/dsa-2404>
- Bulletin de sécurité RedHat RHSA-2012-0370-01 du 07 mars 2012 :  
<https://rhn.redhat.com/errata/RHSA-2012-0370.html>
- Bulletin de sécurité Xen 6 du 02 février 2012 :  
<http://list.xen.org/archives/html/xen-devel/2012-02/msg00212.html>
- Référence CVE CVE-2012-0029 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0029>

## Gestion détaillée du document

**08 février 2012** version initiale.

**09 mars 2012** ajout du bulletin sécurité RedHat.