



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 08 septembre 2011  
N° CERTA-2011-AVI-500

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-2011-AVI-500>

---

### Gestion du document

Référence	CERTA-2011-AVI-500
Titre	Vulnérabilité dans Xen
Date de la première version	08 septembre 2011
Date de la dernière version	–
Source(s)	
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.

## 2 Systèmes affectés

- Xen 3.x ;
- Citrix XenServer 5.0 ;
- Citrix XenServer 5.5 ;
- Citrix XenServer 5.6.

## 3 Résumé

Une vulnérabilité Xen permet à une personne malveillante de provoquer un déni de service du système hôte depuis un système virtualisé.

## 4 Description

Une vulnérabilité, causée par un manque de contrôle lors de l'appel à la version x86\_64 de la macro `__addr_ok()`, permet à une personne malveillante de provoquer l'arrêt inopiné du système hôte depuis un système virtualisé.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Xen OpenWall du 02 septembre 2011 :  
<http://www.openwall.com/lists/oss-security/2011/09/02/2>
- Bulletin de sécurité Citrix CTX130325 du 06 septembre 2011 :  
<http://support.citrix.com/article/CTX130325>
- Référence CVE CVE-2011-2901 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2901>

## **Gestion détaillée du document**

**08 septembre 2011** version initiale.