



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 mai 2011  
N° CERTA-2011-AVI-286

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités 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-286>

---

### Gestion du document

Référence	CERTA-2011-AVI-286
Titre	Vulnérabilités dans Xen
Date de la première version	11 mai 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Xen du 9 mai 2011
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 ;
- atteinte à la confidentialité des données ;
- exécution de code arbitraire ;
- élévation de privilèges.

## 2 Systèmes affectés

- Xen 3.x ;
- Xen 4.x.

## 3 Résumé

Plusieurs vulnérabilités, permettant à une personne malintentionnée de causer un déni de service, porter atteinte à la confidentialité des données, d'élever ses privilèges et d'exécuter du code arbitraire, ont été découvertes dans *Xen*.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *Xen*. Les fonctions de décompression du noyau des machines hôtes ne vérifient pas un certain nombre de paramètres. Cela permet à un utilisateur malintentionné de :

- élever ses privilèges et exécuter du code arbitraire via un dépassement d'entier dans la boucle d'allocation mémoire ;
- accéder à des informations sensibles via la lecture de la mémoire du processus suite à un dépassement d'entier lors du chargement du noyau ;
- causer un déni de service au moyen de la création d'une boucle infini au niveau des outils de gestion.

## 5 Solution

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

## 6 Documentation

- Référence CVE CVE-2011-1583 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1583>
- Bulletin de sécurité *Xen* :  
<http://lists.xensource.com/archives/html/xen-devel/2011-05/msg00483.html>

## Gestion détaillée du document

11 mai 2011 version initiale.