

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Citrix XenServer

---

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-295>

---

### Gestion du document

Référence	CERTA-2011-AVI-295
Titre	Vulnérabilités dans Citrix XenServer
Date de la première version	16 mai 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Citrix CTX129208 et CTX129228 du 11 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

- Dénis de service ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- XenServer 5.0 Update 3 ;
- XenServer 5.5 ;
- XenServer 5.6 ;
- XenServer 5.6 Feature Pack 1.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Citrix XenServer. Elles permettent à un utilisateur malintentionné de provoquer un déni de service ou de porter atteinte à la confidentialité des données.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans Citrix XenServer :

- Plusieurs vulnérabilités non spécifiées permettent à un utilisateur malintentionné disposant des privilèges d'administration sur un système invité de provoquer un déni de service sur l'hyperviseur ;
- une vulnérabilité dans la gestion des journaux permet à un utilisateur d'obtenir une divulgation d'informations d'authentification (XenServer 5.6 uniquement).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Citrix CTX129208 du 11 mai 2011 :  
<http://support.citrix.com/article/CTX129208>
- Bulletin de sécurité Citrix CTX129228 du 11 mai 2011 :  
<http://support.citrix.com/article/CTX129228>

## Gestion détaillée du document

**16 mai 2011** version initiale.