

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Citrix MetaFrame

---

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-2006-AVI-306>

---

### Gestion du document

Référence	CERTA-2006-AVI-306
Titre	Vulnérabilité dans Citrix MetaFrame
Date de la première version	20 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Citrix du 14 juillet 2006
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- Citrix MetaFrame XP 1.0 SP1 et inférieures ;
- Citrix MetaFrame version 1.8 ;
- Citrix MetaFrame Presentation Server version 3.0 ;
- Citrix Presentation Server version 4.0.

Les serveurs Citrix fonctionnant sous Windows Server 2003 ne seraient pas affectés par cette vulnérabilité.

## 3 Résumé

Une vulnérabilité a été identifiée dans certaines versions de Citrix MetaFrame. Elle permettrait à un utilisateur local malveillant d'élever ses privilèges sur le système affecté.

## **4 Description**

Citrix MetaFrame permet la manipulation d'applications par accès distants. Une vulnérabilité a été identifiée dans certaines versions de celui-ci, au moment de son installation : il ajouterait une clé de registre avec des droits d'accès non sécurisés. Une personne malveillante authentifiée peut profiter de cette vulnérabilité pour élever ses privilèges, ou même prendre le contrôle du serveur.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Citrix CTX110492 du 14 juillet 2006 :  
<http://support.citrix.com/article/CTX110492>
- Mises à jour disponibles sur le site Citrix :  
<http://support.citrix.com/hotfixes.jsp>

## **Gestion détaillée du document**

**20 juillet 2006** version initiale.