

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Déni de service sur 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-2001-AVI-122>

---

### Gestion du document

Référence	CERTA-2001-AVI-122
Titre	Déni de service sur Citrix MetaFrame
Date de la première version	19 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité de Citrix
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 initié depuis un système distant.

## 2 Systèmes affectés

Tous les systèmes équipés de Citrix MetaFrame :

- version 1.8 avec le Service Pack 3 ;
- version XP.

## 3 Résumé

Il est possible d'arrêter à distance le service MetaFrame.

## 4 Description

MetaFrame est un complément de Microsoft Terminal Server pour Windows, il permet notamment l'exécution d'applications centralisées depuis n'importe quel type de client.

Un utilisateur mal intentionné peut bloquer le service MetaFrame, puis la machine, en initiant une multitude de connections au serveur.

## 5 Contournement provisoire

Le garde-barrière doit bloquer les ports NetBios (135,137 et 139 en TCP et UDP) ainsi que le port utilisé par MetaFrame (Port 1494/TCP, ICA) pour éviter ce type d'attaque en provenance d'Internet.

## 6 Solution

Télécharger et appliquer le correctif de Citrix selon la version :

- MetaFrame 1.8 Service Pack 3
  - pour Windows NT 4.0 Terminal Server version anglaise : ME183T012
  - pour Windows 2000 en version anglaise : ME183W018
- MetaFrame XP Service Pack 1/Feature Pack 1 : le correctif n'est pas encore disponible.

Sur le site de Citrix :

<http://www.citrix.com/support/>

## 7 Documentation

Avis de sécurité Citrix CTX654124 :

<http://knowledgebase.citrix.com>

## Gestion détaillée du document

19 octobre 2001 version initiale.