

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Citrix Metaframe Presentation

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-2005-ALE-013>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-ALE-013 |
| Titre | Vulnérabilité dans Citrix Metaframe Presentation |
| Date de la première version | 07 octobre 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Citrix #CTX107705 du 27 septembre 2005 |
| Pièce(s) jointe(s) | |

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.

2 Systèmes affectés

- Citrix Metaframe Presentation Server 3.x ;
- Citrix Présentation Server 4.x.

3 Résumé

Une vulnérabilité dans certains produits Citrix permet à un utilisateur mal intentionné de contourner la politique de sécurité.

4 Description

Une vulnérabilité découverte dans la politique de filtrage basée sur la variable `client_name` permet à un utilisateur distant mal intentionné de contourner la politique de sécurité. Une personne malveillante peut s'authentifier auprès du serveur après avoir habilement modifié le fichier `launch.ica`.

5 Contournement provisoire

Changer la politique de sécurité de l'application Citrix de manière à ce que l'authentification ne se fasse pas par le biais de la variable `client name`.

6 Documentation

- Site Internet de l'éditeur :
<http://support.citrix.com>
- Bulletin de sécurité Citrix #CTX107705 du 27 septembre 2005 :
<http://support.citrix.com/kb/entry!default.jspx?categoryID=275&externalID=CTX107705>

Gestion détaillée du document

07 octobre 2005 version initiale.