



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 novembre 2006
N° CERTA-2006-AVI-491

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités de 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-491>

Gestion du document

Référence	CERTA-2006-AVI-491
Titre	Plusieurs vulnérabilités de Citrix MetaFrame
Date de la première version	13 novembre 2006
Date de la dernière version	–
Source(s)	Avis de sécurité Citrix CTX111186 du 08 novembre 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

- Exécution de code arbitraire à distance ;
- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Citrix Presentation Server 4.0 pour Microsoft Windows 2003 ;
- Citrix Presentation Server 4.0 pour Microsoft Windows 2000 ;
- Citrix Presentation Server 4.0 x64 Edition ;
- Citrix MetaFrame Presentation Server 3.0 pour Microsoft Windows 2003 ;
- Citrix MetaFrame Presentation Server 3.0 pour Microsoft Windows 2000 ;
- Citrix MetaFrame XP 1.0 pour Microsoft Windows 2000.

3 Description

Plusieurs vulnérabilités ont été identifiées dans les produits Citrix MetaFrame Presentation Server. Elles concernent le service IMA (pour *Indépendant Management Architecture*), en charge de la communication de serveur à serveur dans le cadre d'une gestion centralisée.

Certains paquets échangés ne seraient pas traités de manière correcte. En particulier, l'une des vulnérabilités impliquerait la fonction `IMA_SECURE_DecryptData1()` dans la bibliothèque `ImaSystem.dll`. Une personne malveillante pourrait donc émettre vers les ports en écoute du service IMA (ports TCP 2512 et 2513 par défaut), afin d'exploiter l'une de ces vulnérabilités. Cela lui permettrait d'interrompre inopinément le service, voire d'exécuter, à distance et sous certaines conditions, des commandes arbitraires.

4 Solution

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

5 Documentation

- Bulletin de sécurité Citrix CTX111186 du 08 novembre 2006 :
<http://support.citrix.com/article/CTX111186>
- Référence CVE CVE-2006-5821 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5821>
- Annonce *Zero Day Initiative* de TippingPoint (3Com) ZDI-06-038 :
<http://www.zerodayinitiative.com/advisories/ZDI-2006-038.html>

Gestion détaillée du document

13 novembre 2006 version initiale.