



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2011
N° CERTA-2011-AVI-419

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des produits Citrix

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-419>

Gestion du document

Référence	CERTA-2011-AVI-419
Titre	Vulnérabilité dans des produits Citrix
Date de la première version	29 juillet 2011
Date de la dernière version	–
Source	Bulletin de sécurité Citrix CTX129430 du 27 juillet 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- XenApp et XenApp Fundamentals, jusqu'à la version 6 ;
- XenDesktop 4, 4 FP 1 et 4 FP 2.

3 Résumé

Une vulnérabilité dans plusieurs produits Citrix permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité est présente dans le programme *ctxmlss.exe*, utilisé par l'interface XML Service des produits Citrix. Elle est exploitable à distance par un utilisateur malveillant non authentifié, au moyen d'un paquet spécialement construit. En cas de succès, l'attaquant peut exécuter du code arbitraire dans le contexte du compte du service Citrix vulnérable.

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 CTX129430 du 27 juillet 2011 :
<http://support/citrix.com/article/CTX129430>

Gestion détaillée du document

29 juillet 2011 version initiale.