Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 août 2011
N° CERTA-2011-AVI-424

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Citrix XenApp et XenDesktop

Gestion du document

Référence	CERTA-2011-AVI-424
Titre	Vulnérabilité dans Citrix XenApp et XenDesktop
Date de la première version	01 août 2011
Date de la dernière version	–
Source(s)	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 ;
- déni de service à distance.

2 Systèmes affectés

- Citrix XenApp versions 6 et antérieures ;
- Citrix XenDesktop versions 4 Feature Pack 2 et antérieures.

3 Résumé

Une vulnérabilité présente dans les applications `Citrix XenApp et XenDesktop` permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans le service `XML` des applications `Citrix XenApp et XenDesktop`. Elle permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire

par le biais d'un paquet construit de façon particulière. Il est à noter qu'une authentification n'est pas nécessaire pour exploiter cette faille.

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

01 août 2011 version initiale.