Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juillet 2007
N° CERTA-2007-AVI-325

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Citrix Access Gateway

Gestion du document

Référence	CERTA-2007-AVI-325
Titre	Multiples vulnérabilités dans Citrix Access Gateway
Date de la première version	20 juillet 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Citrix du 19 juillet 2007
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Citrix Access Gateway versions 4.5.4 et antérieures ;
- toutes les versions inférieures à 4.5 HF1 de Citrix Access Gateway Advanced Edition.

3 Résumé

De multiples vulnérabilités dans les produits `Citrix Access Gateway` permettent à un utilisateur distant d'exécuter du code arbitraire, de contourner la politique de sécurité du système ou de porter atteinte à la confidentialité des données des utilisateurs.

4 Description

Plusieurs vulnérabilités sont présentes dans les produits `Citrix Access Gateway` :

- la première est relative à la façon dont sont stockées les informations des clients et permettrait à un utilisateur local malintentionné d'accéder à la session d'un utilisateur légitime arbitraire ;
- la seconde concerne une erreur de type débordement de mémoire dans certaines bibliothèques de fonctions et permettrait d'exécuter du code arbitraire à distance ;
- la troisième, non précisée par l'éditeur, permettrait à une personne malintentionnée de rediriger sa victime vers un site arbitraire ;
- la dernière vulnŕabilité concerne la console d'administration qui serait vulnérable à des attaques de type « cross-site request forgery » permettant la modification de la configuration d'un périphérique.

5 Contournement provisoire

6 Solution

La version 4.5.5 de `Citrix Access Gateway` et la version 4.5 HF1 de `Citrix Access Gateway Advanced Edition` corrigent le problème :

- http://support.citrix.com/article/CTX114028
- http://support.citrix.com/article/CTX112803

7 Documentation

Bulletins de sécurité `Citrix` du 19 juillet 2007 :

- http://support.citrix.com/article/CTX113814
- http://support.citrix.com/article/CTX113815
- http://support.citrix.com/article/CTX113816
- http://support.citrix.com/article/CTX113817

Gestion détaillée du document

20 juillet 2007 version initiale.