

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Citrix Access Gateway

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-505>

Gestion du document

Référence	CERTA-2006-AVI-505
Titre	Multiples vulnérabilités dans Citrix Access Gateway
Date de la première version	17 novembre 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité Citrix
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Access Gateway Enterprise 4.0 ;
- Access Gateway 4.2 Advanced Edition ;
- Access Gateway appliance 4.2x avec les versions 4.2 et 4.5 d'Access Gateway Advanced Edition.

3 Résumé

De multiples vulnérabilités dans le produit Citrix Access Gateway permettent de contourner la politique de sécurité.

4 Description

Deux vulnérabilités présentes dans le processus d'authentification ainsi que dans l'utilisation de la fonctionnalité Browser-Only d'Access Gateway Enterprise 4.0 et d'Access Gateway 4.2 Advanced

Edition permettent à un utilisateur malintentionné d'accéder à des ressources en contournant la politique de sécurité.

Une vulnérabilité présente dans Access Gateway appliance permet à un utilisateur distant, qui n'est pas authentifié, de compromettre l'intégrité du produit.

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 CTX111695 du 14 novembre 2006 :
<http://support.citrix.com/article/CTX111695>
- Bulletin de sécurité CITRIX CTX111615 du 14 novembre 2006 :
<http://support.citrix.com/article/CTX111615>
- Bulletin de sécurité CITRIX CTX111614 du 14 novembre 2006 :
<http://support.citrix.com/article/CTX111614>

Gestion détaillée du document

17 novembre 2006 version initiale.