



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-396-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Citrix Access Gateway Plug-in

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-396>

Gestion du document

Référence	CERTA-2011-AVI-396-001
Titre	Vulnérabilités dans Citrix Access Gateway Plug-in
Date de la première version	19 juillet 2011
Date de la dernière version	29 juillet 2011
Source(s)	Bulletin de sécurité Citrix CTX129902 du 13 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

- Citrix Access Gateway Plug-in for Windows versions 8.1 antérieures à 8.1-67.7 ;
- Citrix Access Gateway Plug-in for Windows versions 9.0 antérieures à 9.0-70.5 ;
- Citrix Access Gateway Plug-in for Windows versions 9.1 antérieures à 9.1-96.4.

3 Résumé

Des vulnérabilités dans *Citrix Access Gateway Plug-in* permettent d'exécuter du code arbitraire à distance.

4 Description

Des vulnérabilités ont été découvertes dans un composant *ActiveX* de *Citrix Access Gateway Plug-in for Windows*. L'exploitation de ces vulnérabilités, par le biais d'un site Web malveillant, permet l'exécution de code arbitraire à distance.

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 CTX129902 du 13 juillet 2011 :
<http://support.citrix.com/article/CTX129902>
- Référence CVE CVE-2011-2882 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2882>
- Référence CVE CVE-2011-2883 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2883>

Gestion détaillée du document

19 juillet 2011 version initiale.

29 juillet 2011 ajout des références CVE.