Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 novembre 2006
N° CERTA-2006-AVI-398-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Adobe Flash Player

Gestion du document

Référence	CERTA-2006-AVI-398-002
Titre	Vulnérabilité dans Adobe Flash Player
Date de la première version	14 septembre 2006
Date de la dernière version	15 novembre 2006
Source(s)	Bulletin de sécurité Adobe du 12 septembre 2006
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

Adobe Flash Player versions 8.0.24 et antérieures.

3 Description

Plusieurs vulnérabilités ont été identifiées dans le lecteur Adobe Flash Player. Elles permettraient à un utilisateur mal intentionné de contourner les restrictions du paramètre de sécurité `allowScriptAccess`, et d'exécuter du code arbitraire à distance par le biais d'un fichier au format `.swf` construit de façon particulière. Une dernière vulnérabilité concernerait une mauvaise manipulation de chaînes de caractères dynamiques, et de longueur excessive. Elle pourrait provoquer un débordement de mémoire.

Adobe Flash Player es parfois utilisé indirectement, par le biais d'un navigateur Internet, afin de visualiser des contenus animés au format Flash sur un site web.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Adobe du 12 septembre 2006 :
  http://www.adobe.com/support/security/bulletins/apsb06-11.html
- Référence CVE CVE-2006-3014 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2006-3014
- Référence CVE CVE-2006-3311 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2006-3311
- Référence CVE CVE-2006-3587 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2006-3587
- Référence CVE CVE-2006-3588 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2006-3588
- Référence CVE CVE-2006-4640 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2006-4640
- Bulletin de sécurité Microsoft MS06-069 du 14 novembre 2006 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS06-069.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-069.mspx

Gestion détaillée du document

14 septembre 2006 version initiale.
03 octobre 2006 ajout des références CVE.
15 novembre 2006 ajout de la référence au bulletin Microsoft MS06-069.