Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 novembre 2008
N° CERTA-2008-AVI-546

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Adobe Flash Player

Gestion du document

Référence	CERTA-2008-AVI-546
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	07 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB08-20 du 05 novembre 2008
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Adobe Flash Player 9.0.124.0 ainsi que les versions antérieures.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application Adobe Flash Player. L'exploitation de ces dernières permet de contourner la politique de sécurité de l'application (associée à celle du navigateur).

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'application Adobe Flash Player. Certaines de ces vulnérabilités avaient été partiellement corrigées dans la branche 10. D'autres avaient été mentionnées dans le précédent avis CERTA-2008-AVI-512 et le bulletin de sécurité Adobe APSB08-18.

En particulier :

- l'application n'interprète pas correctement certains en-têtes de réponses HTTP. Cette vulnérabilité peut être exploitée pour construire des attaques par injection de code indirecte (*cross-site scripting*) ;
- il serait possible pour un code malveillant de jouer avec la gestion des noms de domaines et la politique d'origine commune mise en oeuvre par les navigateurs pour accéder à des ressources internes (*DNS rebinding*) ;
- l'interprétation des protocoles de la forme `jar:` ne s'effectue pas correctement, sous certaines conditions. Cette vulnérabilité peut être exploitée pour dérober des informations de navigation par exemple.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions corrigeant ces vulnérabilités sont la 9.0.151.0 et la 10.0.12.36.

6 Documentation

- Bulletin de sécurité Adobe apsb08-20 du 05 novembre 2008 :
  http://www.adobe.com/support/security/bulletins/apsb08-20.html
- Avis de sécurité CERTA-2008-AVI-512 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-512/
- Référence CVE CVE-2008-4818 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4818
- Référence CVE CVE-2008-4819 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4819
- Référence CVE CVE-2008-4820 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4820
- Référence CVE CVE-2008-4821 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4821
- Référence CVE CVE-2008-4822 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4822
- Référence CVE CVE-2008-4823 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4823

Gestion détaillée du document

07 novembre 2008 version initiale.