



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2007
N° CERTA-2007-AVI-299

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Adobe Flash Player

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-2007-AVI-299>

Gestion du document

Référence	CERTA-2007-AVI-299
Titre	Vulnérabilités dans Adobe Flash Player
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB07 du 10 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 ;
- attaques de type *cross-site request forgery*.

2 Systèmes affectés

- *Adobe Flash Player* versions 9.0.45.0 et antérieures ;
- *Adobe Flash Player* versions 8.0.34.0 et antérieures ;
- *Adobe Flash Player* versions 7.0.69.0 et antérieures.

3 Résumé

Plusieurs vulnérabilités affectant *Adobe Flash Player* permettent, entre autres, l'exécution de code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans différentes versions de *Adobe Flash Player* :

- une mauvaise validation des données par *Adobe Flash Player* (versions 9.0.45.0 et antérieures) permet, par le biais d'un fichier au format SWF spécifiquement constitué, l'exécution de code arbitraire à distance (référence CVE-2007-3456) ;
- une mauvaise validation du paramètre HTTP `referer` par *Adobe Flash Player* (versions 8.0.34.0 et antérieures, la version 9 n'est pas affectée) permet de réaliser des attaques de type *cross-site request forgery* (référence CVE-2007-3457) ;
- des mises à jour pour les versions Linux et Solaris d'*Adobe Flash Player* version 7 corrigent des vulnérabilités décrites dans le bulletin de sécurité Adobe APSA07-03 (référence CVE-2007-2022).

5 Solution

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

6 Documentation

- Bulletin de sécurité Adobe APSB07-12 du 10 juillet 2007 :
<http://www.adobe.com/support/security/bulletins/apsb07-12.html>
- Bulletin de sécurité Adobe APSA07-03 du 11 avril 2007 :
<http://www.adobe.com/support/security/advisories/apsa07-03.html>
- Référence CVE CVE-2007-3456 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3456>
- Référence CVE CVE-2007-3457 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3457>
- Référence CVE CVE-2007-2022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2022>

Gestion détaillée du document

11 juillet 2007 version initiale.