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 juin 2011
N° CERTA-2011-AVI-342

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Adobe Reader et Acrobat

Gestion du document

Référence	CERTA-2011-AVI-342
Titre	Multiples vulnérabilités dans Adobe Reader et Acrobat
Date de la première version	15 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe apsb11-16 du 15 juin 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

- Adobe Reader X pour Windows, versions 10.x jusqu'à 10.0.1 inclue ;
- Adobe Reader X pour Macintosh, versions 10.x jusqu'à 10.0.3 inclue ;
- Adobe Reader 9 pour Windows et Macintosh, versions 9.x jusqu'à 9.4.4 inclue ;
- Adobe Reader 8 pour Windows et Macintosh, versions 8.x jusqu'à 8.2.6 inclue ;
- Adobe Acrobat X pour Windows et Macintosh, versions 10.x jusqu'à 10.0.3 inclue ;
- Adobe Acrobat 9 pour Windows et Macintosh, versions 9.x jusqu'à 9.4.4 inclue ;
- Adobe Acrobat 8 pour Windows et Macintosh, versions 8.x jusqu'à 8.2.6 inclue.

3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits Adobe Acrobat et Reader. Une large partie d'entre elles permettent à un attaquant de provoquer l'arrêt inopiné de l'application, et pourraient mener à l'exécution de code arbitraire à distance.

4 Description

La mise à jour corrige 13 vulnérabilités dans les produits Adobe Acrobat et Reader:

- quatre d'entre elles permettraient à un attaquant de réaliser l'exécution de code à distance par le biais de dépassement de mémoire tampon (CVE-2011-2094, CVE-2011-2095, CVE-2011-2097) et d'un débordement de tas (CVE-2011-2096) ;
- deux permettraient l'exécution de code arbitraire à distance par corruption de la mémoire (CVE-2011-2098, CVE-2011-2099), une troisième n'affecte que les versions 8.x (CVE-2011-2103) et une quatrième n'affecte que les versions Macintosh des deux produits (CVE-2011-2106) ;
- une erreur dans le chargement de DLL permet l'exécution de code arbitraire à distance (CVE-2011-2100) ;
- certaines entrées ne sont pas suffisamment validées et permettent l'exécution de code par rebond (CVE-2011-2101) ;
- une vulnérabilité non spécifiée n'affectant que les versions 10.x permet le contournement de certaines restrictions (CVE-2011-2102) ;
- deux corruptions de mémoire entrainant une fermeture inopinée ont enfin été corrigées (CVE-2011-2104 et CVE-2011-2105).

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 apsb11-16 du 15 juin 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-16.html
- Référence CVE CVE-2011-2094 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2094
- Référence CVE CVE-2011-2095 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2095
- Référence CVE CVE-2011-2096 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2096
- Référence CVE CVE-2011-2097 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2097
- Référence CVE CVE-2011-2098 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2098
- Référence CVE CVE-2011-2099 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2099
- Référence CVE CVE-2011-2100 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2100
- Référence CVE CVE-2011-2101 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2101
- Référence CVE CVE-2011-2102 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2102
- Référence CVE CVE-2011-2103 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2103
- Référence CVE CVE-2011-2104 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2104
- Référence CVE CVE-2011-2105 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2105
- Référence CVE CVE-2011-2106 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2106

Gestion détaillée du document

15 juin 2011 version initiale.