

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Adobe Acrobat

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-024>

Gestion du document

Référence	CERTA-2007-AVI-024-001
Titre	Multiples vulnérabilités dans Adobe Acrobat
Date de la première version	10 janvier 2007
Date de la dernière version	15 mars 2007
Source(s)	Bulletin de sécurité Adobe du 09 janvier 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

- Attaques de type *Cross Site Scripting* ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Adobe Reader versions 7.0.8 et antérieures ;
- Adobe Acrobat Standard et Professional versions 7.0.8 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans Adobe Reader et Adobe Acrobat permettent des attaques de type *Cross Site Scripting*, un déni de service ou l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités sont présentes dans les produits `Adobe Reader` et `Adobe Acrobat` :

- la première vulnérabilité permet à une personne malveillante de réaliser des attaques de type *Cross Site Scripting* en injectant du code `JavaScript` arbitraire par le biais d'adresses réticulaires (URL) spécialement conçues ;
- la seconde permet à une personne malintentionnée de réaliser un déni de service par le biais d'une adresse réticulaire (URL) spécialement formatée ;
- la troisième permet l'exécution de code arbitraire dans le contexte de l'utilisateur à l'aide d'un fichier PDF spécialement conçu.

5 Solution

Les versions 7.0.9 et 8 corrigent les problèmes. A ce jour, Adobe n'a pas encore mis à disposition un correctif pour `Adobe Reader` et `Adobe Acrobat` version 6.

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

6 Documentation

- Bulletin de sécurité Adobe du 09 janvier 2007 :
<http://www.adobe.com/support/security/bulletins/apsb07-01.html>
- Référence CVE CVE-2007-0048 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0048>
- Référence CVE CVE-2007-0046 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0046>
- Référence CVE CVE-2007-0045 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0045>
- Référence CVE CVE-2006-5857 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5857>
- Bulletin de sécurité GLSA 200701-16 du 22 janvier 2007 de Gentoo :
<http://www.gentoo.org/security/en/glsa/glsa-200701-16.xml>
- Bulletin de sécurité Red Hat RHSA-2007:0017-2 :
<http://rhn.redhat.com/errata/RHSA-2007-0017.html>
- Bulletin de sécurité Red Hat RHSA-2007:0021-2 :
<http://rhn.redhat.com/errata/RHSA-2007-0021.html>
- Bulletin de sécurité Sun Solaris n102847 du 14 mars 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102847-1>
- Bulletin de sécurité SuSE SUSE-SA:2007:011 :
<http://lists.suse.com/archive/suse-security-announce/2007-Jan/0012.html>

Gestion détaillée du document

10 janvier 2007 version initiale.

15 mars 2007 ajout des références à Red Hat, Sun, SuSE, Gentoo.