



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2008
N° CERTA-2008-AVI-541

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Adobe Acrobat et Adobe Reader

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-2008-AVI-541>

Gestion du document

Référence	CERTA-2008-AVI-541
Titre	Multiples vulnérabilités dans Adobe Acrobat et Adobe Reader
Date de la première version	06 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe apsb08-19 du 4 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

- Exécution de code arbitraire à distance ;
- exécution de code arbitraire ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Adobe Acrobat 3D 3.x ;
- Adobe Acrobat 8 Professional ;
- Adobe Acrobat 8.x ;
- Adobe Reader 8.x.

3 Résumé

Plusieurs vulnérabilités affectent les produits Adobe Acrobat et Adobe Reader permettant, entre autres, à une personne malveillante d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans Adobe Acrobat et Adobe Reader :

- plusieurs erreurs dans la validation des données permettent une exécution, locale ou à distance, de code arbitraire ;
- deux erreurs dans le traitement de certaines données par le gestionnaire de téléchargement d'Adobe Reader permettent de modifier les options de sécurité de l'utilisateur pendant le processus de téléchargement ;
- une erreur dans le traitement de données par une méthode *JavaScript* permet une exécution de code arbitraire à distance ;
- une vulnérabilité non documentée permet une élévation de privilèges ;
- une vulnérabilité permet un déni de service via un document *PDF* spécialement conçu.

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 apsb08-19 du 04 novembre 2008 :
<http://www.adobe.com/support/security/bulletins/apsb08-19.html>
- Référence CVE CVE-2008-2549 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2549>
- Référence CVE CVE-2008-2992 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2992>
- Référence CVE CVE-2008-4812 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4812>
- Référence CVE CVE-2008-4813 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4813>
- Référence CVE CVE-2008-4814 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4814>
- Référence CVE CVE-2008-4815 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4815>
- Référence CVE CVE-2008-4816 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4816>
- Référence CVE CVE-2008-4817 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4817>

Gestion détaillée du document

06 novembre 2008 version initiale.