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 octobre 2010
N° CERTA-2010-ALE-014-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Adobe Reader et Adobe Acrobat

Gestion du document

Référence	CERTA-2010-ALE-014-001
Titre	Vulnérabilité dans Adobe Reader et Adobe Acrobat
Date de la première version	09 septembre 2010
Date de la dernière version	06 octobre 2010
Source(s)	Bulletin de sécurité Adobe APSA10-02 du 08 septembre 2010
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 et Adobe Acrobat version 9.3.4 et antérieures, pour toutes plateformes ;
- Adobe Reader et Adobe Acrobat version 8.2.4 et antérieures, pour toutes plateformes.

La vulnérabilité est potentiellement présente sur des versions antérieures de Adobe Reader et Adobe Acrobat.

3 Résumé

L'éditeur a publié un correctif le 5 octobre 2010. Une vulnérabilité affecte Adobe Reader et Adobe Acrobat. Elle permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité dans le module de traitement des polices de caractère d'Adobe Reader et Adobe Acrobat (*CoolType.dll*) permet l'exécution de code arbitraire à distance.

Cette vulnérabilité est actuellement activement exploitée sur l'Internet. Le code d'exploitation semble fonctionner sur de nombreuses plateformes, incluant Microsoft Windows 7 et Vista et a la capacité de contourner les mécanismes de protection de type ASLR (*Address Space Layout Randomization*) et DEP (*Data Execution Prevention*).

5 Contournement provisoire

L'éditeur annonce travailler sur un correctif, qui devrait être publié rapidement. En attendant, le CERTA recommande d'utiliser un lecteur PDF alternatif à jour.

Pour mémoire, plusieurs bonnes pratiques peuvent aider à protéger les utilisateurs :

- s'assurer que les greffons de navigateur permettant d'ouvrir les fichiers PDF n'utilisent pas les logiciels faisant l'objet de cette alerte ;
- désactiver par défaut l'interprétation du JavaScript ;
- utiliser un compte avec des droits limités ;
- convertir les fichiers suspects au format Postscript puis de nouveau au format PDF sur une machine sas ;
- n'ouvrir que des fichiers provenant de sources vérifiées et sûres.

Ces mesures ne sont pas des garanties de protection contre cette vulnérabilité mais peuvent en limiter les impacts.

6 Solution

Les versions d'`Adobe Reader` et `Adobe Acrobat` 9.3.4 et 8.2.4 corrigent cette vulnérabilité. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Document du CERTA CERTA-2010-AVI-470 du 06 octobre 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-470/index.html
- Bulletin de sécurité Adobe APSA10-02 du 08 septembre 2010 :
  http://www.adobe.com/support/security/advisories/apsa10-02.html
- Référence CVE CVE-2010-2883 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2883

Gestion détaillée du document

09 septembre 2010 version initiale.

06 octobre 2010 publication du correctif.