Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2010
N° CERTA-2010-ALE-020-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Adobe Reader et Acrobat

Gestion du document

Référence	CERTA-2010-ALE-020-001
Titre	Vulnérabilité dans Adobe Reader et Acrobat
Date de la première version	05 novembre 2010
Date de la dernière version	17 novembre 2010
Source(s)	Note de sécurité du Adobe PSIRT du 4 novembre 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 ;
- déni de service.

2 Systèmes affectés

Adobe Reader et Acrobat 9.x sur toutes les plateformes.

3 Résumé

L'éditeur a publié, le 16 novembre 2010, un correctif pour Acrobat, sauf sur plateforme Unix, et pour Adobe Reader.

Une vulnérabilité non détaillée affecte le logiciel Adobe Reader. Elle permet le déni de service et l'exécution de code arbitraire.

4 Description

Une vulnérabilité non détaillée affecte les logiciels Adobe Reader et Acrobat. Une personne malintentionnée peut l'exploiter au moyen d'un document spécifiquement réalisé pour provoquer un déni de service ou exécuter du code arbitraire. Une preuve de faisabilité de déni de service est disponible sur l'Internet.

L'exploitation de cette vulnérabilité peut se faire à distance au moyen de greffons dans les navigateurs.

L'éditeur confirme que les versions 8.x d'Adobe Reader et d'Acrobat ne sont pas concernées.

5 Contournement provisoire

Adobe recommande l'utilisation du *JavaScript Blacklist Framework* pour empêcher l'exploitation de la vulnérabilité. Les détails de configuration, en fonction du système, sont disponibles dans la note de sécurité du PSIRT (cf. Documentation).

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 ;
- utiliser un lecteur alternatif.

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

6 Solution

Les versions 9.4.1 d'Adobe Reader et d'Acrobat résolvent ce problème.

La publication du correctif d'Acrobat sur plateforme Unix est annoncée pour le 30 novembre 2010.

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

7 Documentation

- Note de sécurité du Adobe PSIRT du 04 novembre 2010 :
  http://blogs.adobe.com/psirt/2010/11/potential-issue-in-adobe-reader.html
- Bulletin de sécurité Adobe apsb10-28 du 16 novembre 2010 :
  http://www.adobe.com/support/security/bulletins/apsb10-28.html
- Bulletin de sécurité Adobe apsb10-05 du 16 novembre 2010 :
  http://www.adobe.com/support/security/bulletins/apsb10-05.html
- Document du CERTA CERTA-2010-AVI-551 du 17 novembre 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-551/index.html
- Référence CVE CVE-2010-3654 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3654

Gestion détaillée du document

05 novembre 2010 version initiale.

17 novembre 2010 précisions sur la portée et publication de correctifs.