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 avril 2009
N° CERTA-2009-AVI-094-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'interprétation JBIG2 dans le format PDF

Gestion du document

Référence	CERTA-2009-AVI-094-002
Titre	Vulnérabilité dans l'interprétation JBIG2 dans le format PDF
Date de la première version	11 mars 2009
Date de la dernière version	17 avril 2009
Source(s)	Bulletin de sécurité Adobe APSB09-03 du 10 mars 2009 Bulletin de sécurité Adobe APSB09-04 du 18 mars 2009
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 versions 9.x, 8.x et 7.x ;
- Adobe Acrobat Standard, Pro et Pro Extended, versions 9.x, 8.x et 7.x.
- KDE versions antérieures à la version 3.4.5-12 ;
- Xpdf versions antérieures à la mise à jour 3.02pl3.

3 Résumé

Une vulnérabilité dans l'interprétation des documents PDF par différents lecteurs permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une erreur dans différents produits relative à l'interprétation des objets encodés au format JBIG2 dans des fichiers PDF permet à un utilisateur de provoquer l'arrêt du logiciel (*crash*).

Elle permet également l'exécution de code arbitraire sur le système vulnérable avec les droits de l'utilisateur.

L'exploitation de la vulnérabilité ne nécessite pas nécessairement :

- l'intervention de l'utilisateur ;
- l'activation ou la désactivation du support du langage JavaScript.

Certains codes d'exploitation circulant actuellement sur l'Internet sont reconnus par des antivirus sous divers noms : Trojan.Pidief.E, Bloodhound.PDF-6 (Symantec), Exploit-PDF.i (NAI, Mac Afee)...

Certains lecteurs PDF installent une extension permettant à l'explorateur de fichiers de Microsoft Windows de réaliser un aperçu des fichiers au format PDF. De ce fait, la vulnérabilité peut également être exploitée par les méthodes suivantes :

- lors de la sélection d'un fichier PDF exploitant cette vulnérabilité ;
- lors de l'exploration d'un répertoire avec un affichage en mode miniature des icônes.

De plus, il semblerait que cette vulnérabilité puisse être exploitée lors de l'affichage de l'infobulle lié à un fichier PDF malveillant dont les méta-données ont été spécialement construites.

Enfin, l'utilisation de services d'indexation automatique (comme WIS, *Windows Indexing Services*) pourrait déclencher l'exploitation de la vulnérabilité sur un fichier présent sur l'espace de stockage sans intervention particulière de l'utilisateur.

5 Solution

Se référer à la documentation des éditeurs afin d'obtenir les correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Adobe apsb09-03 du 10 mars 2009 :
  http://www.adobe.com/support/security/bulletins/apsb09-03.html
- Bulletin de sécurité Adobe apsb09-04 du 18 mars 2009 :
  http://www.adobe.com/support/security/bulletins/apsb09-04.html
- Avis de sécurité Adobe apsa09-01 du 19 février 2009 :
  http://www.adobe.com/support/security/advisories/apsa09-01.html
- Document du CERTA CERTA-2009-ALE-001 du 20 février 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/index.html
- Bulletin de sécurité Red Hat RSHA-2009-0431 et RSHA-2009-430 du 16 avril 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-0431.html
  http://rhn.redhat.com/errata/RHSA-2009-0430.html
- Mise à jour Xpdf du 30 mars 2009 :
  ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.02pl3.patch
- Référence CVE CVE-2009-0658 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0658
- Référence CVE CVE-2009-0927:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927
- Alerte CERTA-2009-ALE-001 du 20 février 2009:
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/

Gestion détaillée du document

11 mars 2009 version initiale ;

20 mars 2009 ajout des références au bulletin de sécurité APSB09-04 concernant les versions 7.x et 8.x ;

17 avril 2009 ajout des références aux bulletins Red Hat et Xpdf.