Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mars 2009
N° CERTA-2009-ALE-001-005

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans l'interprétation JBIG2 des produits Adobe

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-2009-ALE-001

Gestion du document

Référence	CERTA-2009-ALE-001-005
Titre	Vulnérabilité dans l'interprétation JBIG2 des produits Adobe
Date de la première version	20 février 2009
Date de la dernière version	20 mars 2009
Source(s)	Avis de sécurité Adobe APSA09-01 du 19 février 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.

3 Résumé

Une vulnérabilité dans les produits Adobe permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une erreur dans les produits Adobe relative à l'interprétation des objets encodés au format JBIG2 dans des fichiers PDF permet à un utilisateur de provoquer inopinément 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 Adobe 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)...

L'application Adobe installe 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 Contournement provisoire

L'éditeur Adobe annonce qu'un correctif pour la version 9.x sera disponible le 11 mars 2009.

[11 mars 2009] : L'éditeur a mis à disposition un correctif de sécurité pour les versions 9 de Adobe Reader et Acrobat. Se référer au bulletin de sécurité Adobe apsb09-03 du 10 mars 2009 pour l'obtention des correctifs (cf. section Documentation).

[20 mars 2009] : L'éditeur a mis à disposition un correctif de sécurité pour les versions 8 et 7 de Adobe Reader et Acrobat. Se référer au bulletin de sécurité Adobe apsb09-04 du 18 mars 2009 pour l'obtention des correctifs (cf. section Documentation).

Dans l'attente d'un correctif de l'éditeur, plusieurs mesures peuvent diminuer les risques :
- utiliser un lecteur alternatif à jour. Certains peuvent fermer inopinément à l'ouverture d'un document PDF malveillant mais l'exploitation de la vulnérabilité pour exécuter du code arbitraire n'est pas, à la date de rédaction de ce bulletin, avérée ;
- pour gêner certains codes d'exploitation, désactiver le Javascript dans les lecteur `PDF` Adobe et ne l'activer qu'en cas de stricte nécessité. Cette mesure s'effectue directement dans l'interface de configuration de l'application ou en mettant à 0, pour les systèmes Windows uniquement, la valeur de la variable `bEnableJS` qui se trouve :

```
pour Adobe Reader dans :
        HCU\Software\Adobe\Acrobat Reader\<version>.0\JSPrefs
pour Adobe Acrobat dans :
        HCU\Software\Adobe\Adobe Acrobat\<version>.0\JSPrefs
```

- mettre les pièces jointes au format PDF en quarantaine dans l'attente du correctif.

Par ailleurs, de bonnes pratiques permettent d'atténuer les impacts :
- n'ouvrir que les documents au format PDF provenant d'une source de confiance ;
- travailler avec un compte aux droits limités.

Afin de limiter l'impact d'un fichier `PDF` spécialement construit dans le contexte de l'explorateur de fichiers de Microsoft Windows, le contournement suivant peut être appliqué :

- Après l'avoir sauvegardée, supprimer de la base de registre la clé :
  `HKEY_CLASSES_ROOT\CLSID\{F9DB5320-233E-11D1-9F84-707F02C10627}`

Exemple d'application avec un interpréteur de commandes sous Microsoft Windows :

```
regsvr32 /u ``c:\Program Files\Fichiers communs\Adobe\Acrobat\ActiveX\PDFShell.dll''
```

ou encore :

```
reg export HKCR\CLSID\{F9DB5320-233E-11D1-9F84-707F02C10627} .\export.reg
reg delete HKCR\CLSID\{F9DB5320-233E-11D1-9F84-707F02C10627}
```

6 Solution

Se référer aux bulletins de sécurité Adobe APSB09-03 et APSB09-04 publiés le 10 et le 18 mars respectivement pour l'obtention des correctifs (cf. section Documentation). Le CERTA a émis l'avis CERTA-2009-AVI-094 à ce sujet.

7 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
- Bulletin de sécurité Adobe apsa09-01 du 19 février 2009 :
  http://www.adobe.com/support/security/advisories/apsa09-01.html
- Référence CVE CVE-2009-0658 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0658
- Bulletin de sécurité du CERTA CERTA-2009-AVI-094 du 11 mars 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-094/
- Bulletin d'actualité CERTA-2009-ACT-008, « Vulnérabilité non corrigée dans Adobe Reader » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-008.pdf
- Bulletin d'actualité CERTA-2009-ACT-009, « Retour sur l'alerte CERTA-2009-ALE-001 concernant Adobe » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-009.pdf
- Bulletin d'actualité CERTA-2009-ACT-010, « Retour sur la vulnérabilité PDF » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-010.pdf

Gestion détaillée du document

20 février 2009 version initiale.

23 février 2009 ajout des clés de registre pour la désactivation de l'interprétation JS par GPO.

06 mars 2009 mise à jour de la section «Description» et de la section «Contournement provisoire».

10 mars 2009 ajout des références aux bulletins d'actualité du CERTA.

11 mars 2009 ajout des références aux bulletins de sécurité d'Adobe et du CERTA.

20 mars 2009 ajout des références au dernier bulletin de sécurité d'Adobe APSB09-04.