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 juin 2011
N° CERTA-2011-ALE-003-005

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-003

Gestion du document

Référence	CERTA-2011-ALE-003-005
Titre	Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat
Date de la première version	12 avril 2011
Date de la dernière version	20 juin 2011
Source	Alerte de sécurité Adobe APSA11-02 du 11 avril 2011
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 Flash Player 10.2.153.1 et antérieures sur les systèmes Microsoft Windows, Linux et Oracle Solaris ;
- Adobe Flash Player 10.2.154.25 et antérieures pour les utilisateurs de Chrome ;
- Adobe Flash Player 10.1.156.12 et antérieures sur les systèmes Android ;
- Adobe AIR versions 2.6.19120 et antérieures ;
- le composant *authplay.dll* contenu dans les versions 10.0.2 et antérieures de Adobe Acrobat et Reader pour les systèmes Windows et Macintosh.

3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire à distance affecte des produits Adobe. Elle est actuellement activement exploitée. L'éditeur a publié les correctifs pour toutes les versions concernées.

4 Description

Des produits Adobe sont vulnérables à une faille permettant à une personne malintentionnée d'exécuter du code arbitraire à distance.

L'éditeur rapporte que cette vulnérabilité est actuellement exploitée sur l'Internet, en particulier via des documents Microsoft Word spécialement conçus.

Mise à jour du 14 avril 2011 : l'éditeur annonce les dates de mise à disposition de correctifs suivantes :

- 15 avril 2011 pour Adobe Flash Player 10.2.x (tous les systèmes d'exploitation) ;
- semaine du 25 avril 2011 pour Adobe Reader 9.x, pour Windows et MacOS ;
- semaine du 25 avril pour Adobe Reader X (10.0.1) pour MacOS ;
- 14 juin 2011 pour Adobe Reader X (10.0.2) pour Windows.

5 Contournement provisoire

Il est possible de supprimer ou interdire l'accès à la DLL *authplay.dll*. Le *Protected Mode* inclus dans Adobe Reader X réduit les risques d'exploitation de la vulnérabilité.

Il est également recommandé d'utiliser un logiciel alternatif et à jour en attendant la publication du correctif.

6 Solution

Se référer aux bulletins de sécurité APSB11-07 et APSB11-16 (APSB11-16 inclut les corrections pour les vulnérabilités décrites dans les bulletins APSB11-06 et APSB11-08) de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Adobe APSB11-07 du 15 avril 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-07.html
- Bulletin de sécurité Adobe APSB11-16 du 14 juin 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-16.html
- Bulletin de sécurité Adobe APSB11-08 du 21 avril 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-08.html
- Bulletin d'alerte Adobe APSA11-02 du 11 avril 2011 :
  http://www.adobe.com/support/security/advisories/apsa11-02.html
- Notes de version Google Chrome :
  http://googlechromereleases.blogspot.com/2011/04/stable-channel-update.html
- Avis de sécurité du CERTA CERTA-2011-AVI-234 du 19 avril 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-234/index.html
- Avis de sécurité du CERTA CERTA-2011-AVI-250 du 22 avril 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-250/index.html
- Avis de sécurité du CERTA CERTA-2011-AVI-342 du 15 juin 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-342/index.html
- Référence CVE CVE-2011-0610 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0610
- Référence CVE CVE-2011-0611 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611
- Référence CVE CVE-2011-2094 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2094
- Référence CVE CVE-2011-2095 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2095
- Référence CVE CVE-2011-2096 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2096

- Référence CVE CVE-2011-2097 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2097
- Référence CVE CVE-2011-2098 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2098
- Référence CVE CVE-2011-2099 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2099
- Référence CVE CVE-2011-2100 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2100
- Référence CVE CVE-2011-2101 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2101
- Référence CVE CVE-2011-2102 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2102
- Référence CVE CVE-2011-2103 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2103
- Référence CVE CVE-2011-2104 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2104
- Référence CVE CVE-2011-2105 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2105
- Référence CVE CVE-2011-2106 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2106

Gestion détaillée du document

12 avril 2011 version initiale.

14 avril 2011 annonce des dates de publication des correctifs.

15 avril 2011 ajout du correctif Google Chrome.

19 avril 2011 ajout du bulletin de sécurité Adobe APSB11-07, de Adobe AIR dans les produits vulnérables et de la solution partielle.

22 avril 2011 ajout du bulletin de sécurité Adobe APSB11-08, et des corrections Adobe Reader et Acrobat dans la solution partielle.

20 juin 2011 ajout du bulletin de sécurité Adobe APSB11-16 proposant l'ensemble des correctifs pour Adobe Reader et Acrobat.