

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité Shockwave Flash pour les 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-2010-ALE-007>

Gestion du document

Référence	CERTA-2010-ALE-007-002
Titre	Vulnérabilité Shockwave Flash pour les produits Adobe
Date de la première version	05 juin 2010
Date de la dernière version	30 juin 2010
Source(s)	Avis de sécurité Adobe APSA10-01 du 04 juin 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 ;
- déni de service à distance.

2 Systèmes affectés

- Adobe Reader 9.x ;
- Adobe Acrobat 9.x ;
- Adobe Flash Player 10.0.x.

Cette vulnérabilité peut affecter les systèmes d'exploitation suivants :

- Microsoft Windows ;
- Apple Mac OS X ;
- Gnu/Linux.

3 Résumé

Mise à jour du 30 juin 2010 : cette vulnérabilité est corrigée.

Une vulnérabilité découverte dans certains produits Adobe permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité causée par une erreur dans le traitement des fichiers au format SWF (*Shockwave Flash*) permet à une personne malveillante de provoquer un déni de service de l'application ou d'exécuter du code arbitraire. Cette vulnérabilité peut être exploitée directement au moyen d'un fichier au format SWF spécialement construit, ou indirectement par l'intermédiaire d'un fichier au format PDF contenant un objet SWF malveillant.

Des cas d'exploitation liés à cette vulnérabilité sont d'ores et déjà recensés sur l'Internet.

5 Contournement provisoire

Désactiver l'interprétation des animations Flash ainsi que les animations 3D.

Afin de limiter l'impact lié à l'exploitation de cette vulnérabilité, les contournements décrits ci-dessous, non exhaustifs, peuvent être appliqués.

Remarque : la mise en œuvre de ces contournements de sécurité peut avoir des effets de bord sur l'activité du système. Il est important de les tester avant tout déploiement.

5.1 Mise à jour de sécurité partielle

L'éditeur Adobe a publié un correctif de sécurité pour Adobe Flash Player, la version 10.1.53.64 n'est plus affectée par la vulnérabilité décrite dans ce bulletin d'alerte (cf. Section Documentation).

Dans l'attente d'un correctif de sécurité pour Adobe Reader et Adobe Acrobat, ces applications restent vulnérables.

5.1.1 Adobe Acrobat et Adobe Reader pour Microsoft Windows

- renommer, supprimer ou retirer les droits d'accès du fichier suivant :

```
C:\Program Files\Adobe\Reader 9.0\Reader\authplay.dll
```

5.1.2 Adobe Acrobat et Adobe Reader pour Mac OS X

- renommer, supprimer ou retirer les droits d'accès du fichier suivant :

```
/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/AuthPlayLib.bundle
```

5.1.3 Adobe Acrobat et Adobe Reader pour GNU/Linux

- renommer, supprimer ou retirer les droits d'accès du fichier suivant :

```
/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so
```

Remarque : l'emplacement de ces fichiers peut varier en fonction des distributions GNU/Linux et de la procédure d'installation de l'application.

5.1.4 ActiveX pour Internet Explorer

Désactiver le contrôle ActiveX. Il faut positionner la valeur `Compatibility Flags` pour chaque *Class Identifier* comme décrit ci-dessous :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}]  
"Compatibility Flags"=dword:00000400
```

Class Identifiers à désactiver :

```
{D27CDB6E-AE6D-11cf-96B8-444553540000}  
{D27CDB70-AE6D-11cf-96B8-444553540000}
```

Ou rechercher et supprimer le fichier `flash10*.ocx`.

5.1.5 Module pour Mozilla Firefox

Désactiver le module Shockwave Flash dans le navigateur Mozilla Firefox :

- Dans Outils, puis Modules complémentaires ;
- sélectionner le module Shockwave Flash et le désactiver.

Ou rechercher et supprimer le fichier `flashplayer.xpt`.

5.2 Mise à jour de sécurité complémentaire

Adobe a émis les correctifs pour Adobe Reader et Acrobat le 30 juin 2010.

6 Solution

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

7 Documentation

- Avis de sécurité Adobe apsa10-01 du 04 juin 2010 :
<http://www.adobe.com/support/security/advisories/apsa10-01.html>
- Bulletin de sécurité Adobe apsb10-14 du 10 juin 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-14.html>
- Bulletin de sécurité Adobe apsb10-15 du 29 juin 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>
- Avis CERTA-2010-AVI-261 du 11 juin 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-261/>
- Avis CERTA-2010-AVI-296 du 30 juin 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-296/>
- Référence CVE CVE-2010-1297 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297>

Gestion détaillée du document

05 juin 2010 version initiale.

11 juin 2010 modification de la section Contournement provisoire et de la section Documentation.

30 juin 2010 correctifs pour Adobe Reader et Acrobat.