

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-2009-ALE-013>

Gestion du document

Référence	CERTA-2009-ALE-013-001
Titre	Vulnérabilité Shockwave Flash pour les produits Adobe
Date de la première version	23 juillet 2009
Date de la dernière version	31 juillet 2009
Source(s)	Bloc-notes d'Adobe du 21 juillet 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 ;
- déni de service à distance.

2 Systèmes affectés

- Adobe Acrobat 9.x ;
- Adobe Reader 9.x ;
- Adobe Flash Player 10.x.

Cette vulnérabilité peut affecter les systèmes d'exploitation suivants :

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

3 Résumé

Une vulnérabilité présente 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 malintentionnée de provoquer un déni de service ou d'exécuter du code arbitraire.

Cette vulnérabilité peut être exploitée à distance au moyen d'un fichier SWF ou PDF spécialement construit.

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 Adobe Acrobat et Adobe Reader pour Microsoft Windows

– renommer, supprimer ou retirer les droits d'accès des fichiers suivants :

```
C:\Program Files\Adobe\Reader 9.0\Reader\authplay.dll
C:\Program Files\Adobe\Reader 9.0\Reader\rt3d.dll
```

5.2 Adobe Acrobat et Adobe Reader pour Mac OS X

– renommer, supprimer ou retirer les droits d'accès des fichiers suivants :

```
/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/AuthPlayLib.bundle
/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/Adobe3D.framework
```

5.3 Adobe Acrobat et Adobe Reader pour GNU/Linux

– renommer, supprimer ou retirer les droits d'accès des fichiers suivants :

```
/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so
/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so
```

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

5.4 ActiveX pour Internet Explorer

Désactiver le contrôle ActiveX. Il faut placer 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}
```

Où rechercher et supprimer le fichier flash10*.ocx.

5.5 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.

Où rechercher et supprimer le fichier flashplayer.xpt.

6 Solution

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

7 Documentation

- Bulletin de sécurité Adobe APSA09-03 du 30 juillet 2009 :
<http://www.adobe.com/support/security/bulletins/apsb09-10.html>
- Bulletin de sécurité Adobe APSA09-03 du 22 juillet 2009 :
<http://www.adobe.com/support/security/advisories/apsa09-03.html>
- Bloc-notes d'Adobe du 21 juillet 2009 :
http://blogs.adobe.com/psirt/2009/07/potential_adobe_reader_and fla.html
- Note de vulnérabilité de l'US-CERT VU#259425 du 22 juillet 2009 :
<http://www.kb.cert.org/vuls/id/259425>
- Avis CERTA-2009-AVI-305 du 31 juillet 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-305/index.html>
- Référence CVE CVE-2009-1862 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1862>

Gestion détaillée du document

23 juillet 2009 version initiale ;

31 juillet 2009 ajout de la solution.