Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 octobre 2010
N° CERTA-2010-ALE-016-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité Adobe Shockwave Player

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-016

Gestion du document

Référence	CERTA-2010-ALE-016-001
Titre	Vulnérabilité Adobe Shockwave Player
Date de la première version	22 octobre 2010
Date de la dernière version	29 octobre 2010
Source(s)	Bulletin de sécurité Adobe du 21 octobre 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 Shockwave Player 11.5.8.612 et antérieures.

Cette vulnérabilité peut affecter les systèmes d'exploitation suivants :

- Microsoft Windows ;
- Apple Mac OS X.

3 Résumé

Une vulnérabilité découverte dans `Adobe Shockwave Player` permet à un utilisateur de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité causée par une erreur dans le traitement des fichiers au format *DIR* a été découverte dans `Adobe Shockwave Player`. Elle permet à une personne malveillante distante de provoquer un déni de service ou d'exécuter du code arbitraire. Cette vulnérabilité peut être exploitée au moyen d'un fichier DIR spécialement construit, via un navigateur Internet mais d'autres vecteurs d'exploitation sont envisageables.

5 Contournement provisoire

Ces contournements provisoires ne sont plus d'actualité, un correctif étant disponible

Désactiver `Shockwave Player`.

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 oeuvre de ces contournements de sécurité peut avoir des effets de bords sur l'activité du système. Il est important de les tester avant tout déploiement.

5.1 ActiveX pour Internet Explorer

Désactiver le contrôle ActiveX. Il faut positionner la valeur `Compatibility Flags` pour le *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 Identifier à désactiver :

```
{233C1507-6A77-46A4-9443-F871F945D258}
```

5.2 Module pour Mozilla Firefox

Désactiver le module `Shockwave for Director` dans le navigateur de Mozilla Firefox :

- Dans `Outils`, puis `Modules complémentaires` ;
- sélectionner le module `Shockwave for Director` et le désactiver.

6 Solution

Se référer au bulletin de sécurité Adobe APSB10-25 du 28 octobre 2010 pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Adobe APSB10-25 du 28 ocotbre 2010 :
  http://www.adobe.com/support/security/bulletins/apsb10-25.html
- Bulletin de sécurité Adobe APSA10-04.html du 21 octobre 2010 :
  http://www.adobe.com/support/security/advisories/apsa10-04.html
- Avis CERTA-2010-AVI-523 du 29 octobre 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-523/index.html
- Référence CVE CVE-2010-3653 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3653

Gestion détaillée du document

22 octobre 2010 version initiale.

29 octobre 2010 ajout du correctif.