



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 novembre 2009  
N° CERTA-2009-AVI-472

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-2009-AVI-472>

---

### Gestion du document

Référence	CERTA-2009-AVI-472
Titre	Multiples vulnérabilités dans Adobe Shockwave Player
Date de la première version	04 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB09-16 du 03 novembre 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 Shockwave Player 11.5.1.601 et les versions précédentes.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Adobe Shockwave Player permettant à une personne distante malintentionnée d'exécuter du code arbitraire ou d'effectuer un déni de service.

## 4 Description

De multiples vulnérabilités dans Adobe Shockwave Player ont été découvertes :

- une erreur d'index permet d'exécuter du code arbitraire à distance (CVE-2009-3463) ;

- une erreur de pointeur permet d'exécuter du code arbitraire à distance (CVE-2009-3464 et CVE-2009-3465);
- une erreur dans la résolution de la taille d'une chaîne de caractères permet d'exécuter du code arbitraire à distance (CVE-2009-3466);
- une erreur dans la gestion de certaines bornes permet de provoquer un déni de service (CVE-2009-3244).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Adobe apsb09-16 du 03 novembre 2009 :  
<http://www.adobe.com/support/security/bulletins/apsb09-16.html>
- Référence CVE CVE-2009-3244 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3244>
- Référence CVE CVE-2009-3463 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3463>
- Référence CVE CVE-2009-3464 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3464>
- Référence CVE CVE-2009-3465 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3465>
- Référence CVE CVE-2009-3466 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3466>

## Gestion détaillée du document

**04 novembre 2009** version initiale.