



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 mai 2011  
N° CERTA-2011-AVI-290

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Adobe Flash 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-2011-AVI-290>

---

### Gestion du document

Référence	CERTA-2011-AVI-290
Titre	Vulnérabilités dans Adobe Flash Player
Date de la première version	13 mai 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB11-12 du 12 mai 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 10.2.159.1 et versions antérieures pour les systèmes d'exploitation Windows, Macintosh, Linux et Solaris ;
- Adobe Flash Player 10.2.154.28 et versions antérieures pour Google Chrome ;
- Adobe Flash Player 10.2.157.51 et versions antérieures pour Google Android.

## 3 Résumé

Plusieurs vulnérabilités permettant l'exécution de code arbitraire à distance affectent *Adobe Flash Player*.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans *Adobe Flash Player*. Ces vulnérabilités peuvent être exploitées par une personne malveillante distante pour provoquer de l'exécution de code arbitraire à l'aide d'un

fichier Flash (SWF) spécialement conçu. Ce fichier peut également être contenu dans d'autres formats de fichiers (Microsoft Word, Microsoft Excel, ...).

## 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 apsb11-12 du 12 mai 2011 :  
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>
- Référence CVE CVE-2011-0579 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0579>
- Référence CVE CVE-2011-0618 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0618>
- Référence CVE CVE-2011-0619 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0619>
- Référence CVE CVE-2011-0620 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0620>
- Référence CVE CVE-2011-0621 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0621>
- Référence CVE CVE-2011-0622 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0622>
- Référence CVE CVE-2011-0623 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0623>
- Référence CVE CVE-2011-0624 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0624>
- Référence CVE CVE-2011-0625 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0625>
- Référence CVE CVE-2011-0626 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0626>
- Référence CVE CVE-2011-0627 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0627>
- Référence CVE CVE-2011-0628 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0628>

## Gestion détaillée du document

13 mai 2011 version initiale.