



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 novembre 2009
N° CERTA-2009-AVI-516

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-AVI-516>

Gestion du document

Référence	CERTA-2009-AVI-516
Titre	Multiples vulnérabilités dans les produits Adobe
Date de la première version	26 novembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Adobe
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Adobe AIR 1.x ;
- Adobe Flash Player 10.x ;
- Adobe Flash Player 9.x.

3 Résumé

Plusieurs vulnérabilités présentes dans les lecteurs Flash d'Adobe permettent de contourner la politique de sécurité, de porter atteinte à l'intégrité des données, ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités, notamment de type débordement de mémoire ou pointeur nul, peuvent être exploitées par une personne malveillante afin d'exécuter du code arbitraire à distance au moyen d'un fichier au format `swf` spécialement construit.

5 Solution

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

6 Documentation

- Bulletin de sécurité Adobe apsa09-03 du 02 août 2009 :
<http://www.adobe.com/support/security/advisories/apsa09-03.html>
- Bulletin de sécurité Adobe apsa09-04 du 30 juillet 2009 :
<http://www.adobe.com/support/security/advisories/apsa09-04.html>
- Bulletin de sécurité Adobe apsb09-10 du 09 septembre 2009 :
<http://www.adobe.com/support/security/bulletins/apsb09-10.html>
- Référence CVE CVE-2009-0901 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0901>
- Référence CVE CVE-2009-1862 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1862>
- Référence CVE CVE-2009-1863 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1863>
- Référence CVE CVE-2009-1864 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1864>
- Référence CVE CVE-2009-1865 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1865>
- Référence CVE CVE-2009-1866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1866>
- Référence CVE CVE-2009-1867 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1867>
- Référence CVE CVE-2009-1868 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1868>
- Référence CVE CVE-2009-1869 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1869>
- Référence CVE CVE-2009-1870 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1870>
- Référence CVE CVE-2009-2395 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2395>
- Référence CVE CVE-2009-2493 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493>

Gestion détaillée du document

26 novembre 2009 version initiale.