



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mars 2011
N° CERTA-2011-ALE-002-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat

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-ALE-002>

Gestion du document

Référence	CERTA-2011-ALE-002-002
Titre	Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat
Date de la première version	15 mars 2011
Date de la dernière version	22 mars 2011
Source(s)	Bulletin de sécurité Adobe APSA11-01 du 14 mars 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 10.2.152.33 et antérieures sur les systèmes Windows, Linux et Solaris ;
- Adobe Flash Player 10.2.154.18 et antérieures pour les utilisateurs de Chrome ;
- Adobe Flash Player 10.1.106.16 et antérieures sur les systèmes Android ;
- le composant *authplay.dll* contenu dans les versions 10.0.1 et antérieures de Adobe Acrobat et Reader.

3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire à distance affecte des produits Adobe. Elle est actuellement activement exploitée. L'éditeur propose des correctifs depuis le 22 mars 2011.

4 Description

Une vulnérabilité affecte des produits Adobe. Elle permet à une personne malintentionnée d'exécuter du code arbitraire à distance. Elle est actuellement activement exploitée sur l'Internet, notamment par le biais de fichiers Microsoft Excel spécialement conçus.

5 Contournement provisoire

Il est possible de supprimer ou interdire l'accès au composant *authplay.dll*. Cela empêchera l'exécution du contenu Flash et provoquera une erreur lors de l'ouverture de documents ayant un tel contenu.

Un moyen de contournement pour les utilisateurs de Windows est l'installation du Microsoft's Enhanced Mitigation Evaluation Toolkit (EMET). Cet outil permet d'activer un certain nombre de protections pour les applications exécutables sélectionnées. Dans le cadre de cette vulnérabilité, il est intéressant de l'activer pour les applications Microsoft Office (en priorité Excel) et pour le navigateur Web. Ces protections comprennent Data Execution Prevention (DEP), Export Address Table Access Filtering (EAF), et HeapSpray pre-allocation. Ces mesures de protection se sont montrées efficaces contre les attaques connues utilisant cette vulnérabilité, notamment parce que ces dernières utilisent la méthode HeapSpray pour se stabiliser.

6 Solution

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

7 Documentation

- Bulletin de sécurité Adobe Flash apsb11-05 du 21 mars 2011 :
<http://www.adobe.com/support/security/bulletins/apsb11-05.html>
- Bulletin de sécurité Adobe Reader et Acrobat apsb11-06 du 21 mars 2011 :
<http://www.adobe.com/support/security/bulletins/apsb11-06.html>
- Bulletin de sécurité Adobe apsa11-01 du 14 mars 2011 :
<http://www.adobe.com/support/security/advisories/apsa11-01.html>
- Référence CVE CVE-2011-0609 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609>
- Correctif Google Chrome :
<http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95414>

Gestion détaillée du document

15 mars 2011 version initiale.

18 mars 2011 ajout du correctif Chrome et modification de la section des contournements provisoires.

22 mars 2011 ajout des liens vers les bulletins proposant le téléchargement des correctifs.