



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juin 2013
N° CERTA-2013-AVI-348

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2013-AVI-348>

Gestion du document

Référence	CERTA-2013-AVI-348
Titre	Vulnérabilité dans Adobe Flash Player
Date de la première version	12 juin 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB13-16 du 11 juin 2013
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(s)

- exécution de code arbitraire à distance

2 Systèmes affectés

- Adobe Flash Player versions 11.7.700.202 et antérieures pour Windows
- Adobe Flash Player versions 11.7.700.203 et antérieures pour Macintosh
- Adobe Flash Player versions 11.2.202.285 et antérieures pour Linux
- Adobe Flash Player versions 11.1.115.58 et antérieures pour Android 4.x
- Adobe Flash Player versions 11.1.111.54 et antérieures pour Android 3.x et 2.x
- Adobe AIR versions 3.7.0.1860 et antérieures pour Windows et Macintosh
- Adobe AIR versions 3.7.0.1860 et antérieures pour Android
- Adobe AIR SDK et Compilateur versions 3.7.0.1860 et antérieures

3 Résumé

Une vulnérabilité a été corrigée dans *Adobe Flash Player*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Adobe APSB13-16 du 11 juin 2013
<http://www.adobe.com/support/security/bulletins/apsb13-16.html>
- Référence CVE CVE-2013-3343
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3343>

Gestion détaillée du document

12 juin 2013 version initiale.