

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2010-AVI-538>

Gestion du document

Référence	CERTA-2010-AVI-538
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	05 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB10-26 du 04 novembre 2010
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Adobe Flash Player 10.1.85.3 et versions antérieures pour Windows, Macintosh, Linux et Solaris ;
- Adobe Flash Player 10.1.95.1 pour Android.

3 Résumé

De multiples vulnérabilités dans Adobe Flash Player permettent, entre autre, à une personne distante malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités dans Adobe Flash Player ont été découvertes :

- Plusieurs corruptions de la mémoire permettent d'exécuter du code arbitraire à distance (CVE-2010-3654, CVE-2010-3637, CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, CVE-2010-3652);
- une erreur de validation permet de contourner la politique de restriction d'accès à certains fichiers (CVE-2010-3636);
- une vulnérabilité permettant de porter atteinte à la confidentialité des données existe dans la version Macintosh pour le navigateur Safari du lecteur (CVE-2010-3638);
- une vulnérabilité permet de provoquer à minima un déni de service (CVE-2010-3639).

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 APSB10-26 du 04 novembre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>
- Référence CVE CVE-2010-3636 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3636>
- Référence CVE CVE-2010-3637 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3637>
- Référence CVE CVE-2010-3638 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3638>
- Référence CVE CVE-2010-3639 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3639>
- Référence CVE CVE-2010-3640 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3640>
- Référence CVE CVE-2010-3641 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3641>
- Référence CVE CVE-2010-3642 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3642>
- Référence CVE CVE-2010-3643 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3643>
- Référence CVE CVE-2010-3644 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3644>
- Référence CVE CVE-2010-3645 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3645>
- Référence CVE CVE-2010-3646 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3646>
- Référence CVE CVE-2010-3647 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3647>
- Référence CVE CVE-2010-3648 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3648>
- Référence CVE CVE-2010-3649 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3649>
- Référence CVE CVE-2010-3650 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3650>
- Référence CVE CVE-2010-3652 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3652>

- Référence CVE CVE-2010-3654 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3654>
- Référence CVE CVE-2010-3976 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3976>

Gestion détaillée du document

05 novembre 2010 version initiale.