Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 mars 2009
N° CERTA-2009-AVI-076-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités d'Adobe Flash Player

Gestion du document

Référence	CERTA-2009-AVI-076-001
Titre	Vulnérabilités d'Adobe Flash Player
Date de la première version	25 février 2009
Date de la dernière version	06 mars 2009
Source(s)	Bulletin de sécurité Adobe APSB09-01 du 24 février 2009
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

- Déni de service à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Adobe Flash Player, version 10.0.12.36 et versions précédentes ;
- Adobe Flash Player, version 10.0.15.3 pour Linux et versions précédentes.

3 Résumé

Plusieurs vulnérabilités affectent le lecteur multimédia Adobe Flash Player. Certaines d'entre elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent le lecteur multimédia Adobe Flash Player :

- la première concerne le module *Settings Manager*. L'exploitation de cette vulnérabilité sous forme de détournement de clic (*clickjacking*) permet à un utilisateur malveillant d'exécuter du code arbitraire sur le système vulnérable ;
- un défaut de validation des données entrées permet à un utilisateur malveillant de provoquer un arrêt inopiné du lecteur ;
- un problème permet de provoquer un débordement de tampon. Son exploitation pour exécuter du code arbitraire à distance serait possible ;
- sur les plateformes Linux, un défaut permet à un utilisateur malveillant de lire des données et d'élever ses privilèges ;
- sur les plateformes Windows, la gestion défectueuse du pointeur de souris permet à un utilisateur malveillant de réaliser du *clickjacking*. Cette exploitation permet à un utilisateur malveillant d'exécuter du code arbitraire sur le système vulnérable.

5 Solution

La version 10.0.22.87 remédie à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Adobe APSB09-01 du 24 février 2009 :
  http://www.adobe.com/support/security/bulletins/apsb09-01.html
- Bulletin d'actualité du CERTA du 10 octobre 2008, section 3 :
  http://www.certa.ssi.gouv.fr//site/CERTA-2008-ACT-041/index.html
- Bulletin de sécurité Red Hat RHSA-2009:0332 du 25 février 2009 :
  http://rhn.redhat.com/errata/RHSA-2008-0332.html
- Bulletin de sécurité Red Hat RHSA-2009:0334 du 25 février 2009 :
  http://rhn.redhat.com/errata/RHSA-2008-0334.html
- Bulletin de sécurité SuSE SuSE-SA:2009:011 du 26 février 2009 :
  http://lists.opensuse.org/opensuse-security-announce/2009-02/msg00004.html
- Référence CVE CVE-2009-0114 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0114
- Référence CVE CVE-2009-0519 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0519
- Référence CVE CVE-2009-0520 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0520
- Référence CVE CVE-2009-0521 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0521
- Référence CVE CVE-2009-0522 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0522

Gestion détaillée du document

25 février 2009 version initiale.
06 mars 2009 ajout des références aux bulletins de sécurité Red Hat et SuSE.