Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 13 décembre 2016
N° CERTFR-2016-AVI-410

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Adobe Flash Player

Gestion du document

Référence	CERTFR-2016-AVI-410
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	13 décembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe apsb16-39 du 13 décembre 2016
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
- contournement de la politique de sécurité

2 - Systèmes affectés

- Adobe Flash Player Desktop Runtime versions antérieures à 24.0.0.186 sur Windows et Macintosh
- Adobe Flash Player pour Google Chrome versions antérieures à 24.0.0.186 sur Windows, Macintosh, Linux et Chrome OS
- Adobe Flash Player pour Microsoft Edge and Internet Explorer 11 versions antérieures à 24.0.0.186 sur Windows 10 et 8.1
- Adobe Flash Player pour Linux versions antérieures à 24.0.0.186 sur Linux

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Adobe Flash Player*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité.
Adobe indique que la vulnérabilité CVE-2016-7892 est activement exploitée, dans le cadre d'attaques ciblées, contre des utilisateurs d'Internet Explorer(32-bit) sur Windows.

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 apsb16-39 du 13 décembre 2016
  https://helpx.adobe.com/security/products/flash-player/apsb16-39.html
- Référence CVE CVE-2016-7867
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7867
- Référence CVE CVE-2016-7868
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7868
- Référence CVE CVE-2016-7869
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7869
- Référence CVE CVE-2016-7870
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7870
- Référence CVE CVE-2016-7871
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7871
- Référence CVE CVE-2016-7872
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7872
- Référence CVE CVE-2016-7873
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7873
- Référence CVE CVE-2016-7874
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7874
- Référence CVE CVE-2016-7875
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7875
- Référence CVE CVE-2016-7876
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7876
- Référence CVE CVE-2016-7877
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7877
- Référence CVE CVE-2016-7878
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7878
- Référence CVE CVE-2016-7879
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7879
- Référence CVE CVE-2016-7880
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7880
- Référence CVE CVE-2016-7881
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7881
- Référence CVE CVE-2016-7890
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7890
- Référence CVE CVE-2016-7892
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7892

Gestion détaillée du document

13 décembre 2016 version initiale.