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 10 mars 2016
N° CERTFR-2016-AVI-094

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Adobe Flash Player

Gestion du document

Référence	CERTFR-2016-AVI-094
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	10 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe apsb16-08 du 10 mars 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

2 - Systèmes affectés

- Adobe Flash Player versions antérieures à 21.0.0.182 pour Windows et Macintosh
- Adobe Flash Player ESR versions antérieures à 18.0.0.333 pour Windows et Macintosh
- Adobe Flash Player pour Google Chrome versions antérieures à 21.0.0.182 pour Windows, Macintosh, Linux et ChromeOS
- Adobe Flash Player pour Internet Explorer et Edge versions antérieures à 21.0.0.182 pour Windows
- Adobe Flash Player versions antérieures à 11.2.202.577 pour Linux
- Adobe AIR versions antérieures à 21.0.0.176 pour Windows et Macintosh
- Adobe AIR SDK versions antérieures à 21.0.0.176 pour Windows, Macintosh, Android et iOS
- Adobe AIR versions antérieures à 21.0.0.176 pour Android

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.

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 apsb16-08 du 10 mars 2016
  https://helpx.adobe.com/security/products/flash-player/apsb16-08.html
- Référence CVE CVE-2016-0960
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0960
- Référence CVE CVE-2016-0961
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0961
- Référence CVE CVE-2016-0962
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0962
- Référence CVE CVE-2016-0963
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0963
- Référence CVE CVE-2016-0986
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0986
- Référence CVE CVE-2016-0987
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0987
- Référence CVE CVE-2016-0988
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0988
- Référence CVE CVE-2016-0989
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0989
- Référence CVE CVE-2016-0990
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0990
- Référence CVE CVE-2016-0991
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0991
- Référence CVE CVE-2016-0993
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0993
- Référence CVE CVE-2016-0994
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0994
- Référence CVE CVE-2016-0995
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0995
- Référence CVE CVE-2016-0996
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0996
- Référence CVE CVE-2016-1000
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1000
- Référence CVE CVE-2016-1001
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1001
- Référence CVE CVE-2016-1005
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1005
- Référence CVE CVE-2016-1010
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1010

Gestion détaillée du document

10 mars 2016 version initiale.