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 12 novembre 2014
N° CERTFR-2014-AVI-478

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Adobe Flash Player

Gestion du document

Référence	CERTFR-2014-AVI-478
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	12 novembre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB14-24 du 11 novembre 2014
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
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Adobe Flash Player à partir de la version 15.0.0.189 pour Windows et Macintosh
- Adobe Flash Player à partir de la version 13.0.0.250 pour Windows et Macintosh
- Adobe Flash Player pour Google Chrome à partir de la version 15.0.0.189 pour Windows, Macintosh et Linux
- Adobe Flash Player pour Internet Explorer 10 et 11 à partir de la version 15.0.0.189 pour Windows 8 et 8.1
- Adobe Flash Player à partir de la version 11.2.202.411 pour Linux
- Adobe AIR à partir de la version 15.0.0.293 pour Windows et Macintosh
- Adobe AIR pour Android à partir de la version 15.0.0.293
- Adobe AIR SDK à partir de la version 15.0.0.302 pour Windows, Macintosh, Android et iOS
- Adobe AIR SDK et Compilateur à partir de la version 15.0.0.302 pour Windows, Macintosh, Android et iOS

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, une atteinte à la confidentialité des données et une élévation de privilèges.

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 APSB14-24 du 11 novembre 2014
  https://helpx.adobe.com/security/products/flash-player/apsb14-24.html
- Référence CVE CVE-2014-0573
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0573
- Référence CVE CVE-2014-0574
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0574
- Référence CVE CVE-2014-0576
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0576
- Référence CVE CVE-2014-0577
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0577
- Référence CVE CVE-2014-0581
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0581
- Référence CVE CVE-2014-0582
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0582
- Référence CVE CVE-2014-0583
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0583
- Référence CVE CVE-2014-0584
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0584
- Référence CVE CVE-2014-0585
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0585
- Référence CVE CVE-2014-0586
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0586
- Référence CVE CVE-2014-0588
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0588
- Référence CVE CVE-2014-0589
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0589
- Référence CVE CVE-2014-0590
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0590
- Référence CVE CVE-2014-8437
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8437
- Référence CVE CVE-2014-8438
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8438
- Référence CVE CVE-2014-8440
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8440
- Référence CVE CVE-2014-8441
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8441
- Référence CVE CVE-2014-8442
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8442

Gestion détaillée du document

12 novembre 2014 version initiale.