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 février 2016
N° CERTFR-2016-AVI-054

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Adobe

Gestion du document

Référence	CERTFR-2016-AVI-054
Titre	Multiples vulnérabilités dans les produits Adobe
Date de la première version	10 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB16-04 du 09 février 2016 Bulletin de sécurité Adobe APSB16-03 du 09 février 2016 Bulletin de sécurité Adobe APSB16-05 du 09 février 2016 Bulletin de sécurité Adobe APSB16-07 du 09 février 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
- atteinte à la confidentialité des données
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Adobe Flash Player versions antérieures à 20.0.0.306 pour Windows et Macintosh
- Adobe Flash Player ESR versions antérieures à 18.0.0.329 pour Windows et Macintosh
- Adobe Flash Player versions antérieures à 11.2.202.569 pour Linux
- AIR SDK versions antérieures à 20.0.0.260 pour Windows, Macintosh, Android et iOS
- AIR SDK & Compiler versions antérieures à 20.0.0.260 pour Windows, Macintosh, Android et iOS
- Adobe Photoshop CC 2015 versions antérieures à 16.1.2 (2015.1.2) pour Windows et Macintosh
- Adobe Photoshop CC 2014 versions antérieures à 15.2.4 (2014.2.4) pour Windows et Macintosh
- Adobe Bridge CC versions antérieures à 6.2 pour Windows et Macintosh
- Adobe Experience Manager versions 6.1.0, 6.0.0, et 5.6.1 pour Windows, Unix, Linux et OS X
- Adobe Connect versions antérieures à 9.5.2 pour Windows

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Adobe*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

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 APSB16-04 du 09 février 2016
  https://helpx.adobe.com/security/products/flash-player/apsb16-04.html
- Bulletin de sécurité Adobe APSB16-03 du 09 février 2016
  https://helpx.adobe.com/security/products/photoshop/apsb16-03.html
- Bulletin de sécurité Adobe APSB16-05 du 09 février 2016
  https://helpx.adobe.com/security/products/experience-manager/apsb16-05.html
- Bulletin de sécurité Adobe APSB16-07 du 09 février 2016
  https://helpx.adobe.com/security/products/connect/apsb16-07.html
- Référence CVE CVE-2016-0948
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0948
- Référence CVE CVE-2016-0949
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0949
- Référence CVE CVE-2016-0950
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0950
- Référence CVE CVE-2016-0951
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0951
- Référence CVE CVE-2016-0952
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0952
- Référence CVE CVE-2016-0953
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0953
- Référence CVE CVE-2016-0955
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0955
- Référence CVE CVE-2016-0956
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0956
- Référence CVE CVE-2016-0957
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0957
- Référence CVE CVE-2016-0958
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0958
- Référence CVE CVE-2016-0964
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0964
- Référence CVE CVE-2016-0965
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0965
- Référence CVE CVE-2016-0966
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0966
- Référence CVE CVE-2016-0967
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0967
- Référence CVE CVE-2016-0968
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0968
- Référence CVE CVE-2016-0969
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0969
- Référence CVE CVE-2016-0970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0970

- Référence CVE CVE-2016-0971
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0971
- Référence CVE CVE-2016-0972
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0972
- Référence CVE CVE-2016-0973
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0973
- Référence CVE CVE-2016-0974
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0974
- Référence CVE CVE-2016-0975
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0975
- Référence CVE CVE-2016-0976
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0976
- Référence CVE CVE-2016-0977
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0977
- Référence CVE CVE-2016-0978
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0978
- Référence CVE CVE-2016-0979
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0979
- Référence CVE CVE-2016-0980
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0980
- Référence CVE CVE-2016-0981
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0981
- Référence CVE CVE-2016-0982
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0982
- Référence CVE CVE-2016-0983
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0983
- Référence CVE CVE-2016-0984
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0984
- Référence CVE CVE-2016-0985
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0985

Gestion détaillée du document

10 février 2016 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-054`