

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Adobe Flash Player

Gestion du document

Référence	CERTFR-2016-AVI-170
Titre	Multiples vulnérabilités dans Adobe Flash Player
Date de la première version	12 mai 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB16-15 du 12 mai 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 Desktop Runtime versions antérieures à 21.0.0.242 sur Windows et Macintosh
- Adobe Flash Player ESR versions antérieures à 18.0.0.352 sur Windows et Macintosh
- Adobe Flash Player pour Google Chrome versions antérieures à 21.0.0.242 sur Windows, Macintosh, Linux et ChromeOS
- Adobe Flash Player pour Microsoft Edge et Internet Explorer 11 versions antérieures à 21.0.0.242 sur Windows 10 et 8.1
- Adobe Flash Player pour Linux versions antérieures à 11.2.202.616 sur Linux
- AIR Desktop Runtime versions antérieures à 21.0.0.215 sur Windows et Macintosh
- AIR SDK versions antérieures à 21.0.0.215 sur Windows, Macintosh, Android et iOS
- AIR SDK & Compiler versions antérieures à 21.0.0.215 sur 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.

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 APSB16-15 du 12 mai 2016
<https://helpx.adobe.com/security/products/flash-player/apsb16-15.html>
- Référence CVE CVE-2016-1096
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1096>
- Référence CVE CVE-2016-1097
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1097>
- Référence CVE CVE-2016-1098
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1098>
- Référence CVE CVE-2016-1099
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1099>
- Référence CVE CVE-2016-1100
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1100>
- Référence CVE CVE-2016-1101
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1101>
- Référence CVE CVE-2016-1102
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1102>
- Référence CVE CVE-2016-1103
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1103>
- Référence CVE CVE-2016-1104
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1104>
- Référence CVE CVE-2016-1105
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1105>
- Référence CVE CVE-2016-1106
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1106>
- Référence CVE CVE-2016-1107
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1107>
- Référence CVE CVE-2016-1108
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1108>
- Référence CVE CVE-2016-1109
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1109>
- Référence CVE CVE-2016-1110
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1110>
- Référence CVE CVE-2016-4108
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4108>
- Référence CVE CVE-2016-4109
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4109>
- Référence CVE CVE-2016-4110
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4110>
- Référence CVE CVE-2016-4111
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4111>
- Référence CVE CVE-2016-4112
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4112>
- Référence CVE CVE-2016-4113
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4113>
- Référence CVE CVE-2016-4114
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4114>
- Référence CVE CVE-2016-4115
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4115>

- Référence CVE CVE-2016-4116
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4116>
- Référence CVE CVE-2016-4117
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4117>

Gestion détaillée du document

12 mai 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-170>
