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 03 août 2016
N° CERTFR-2016-AVI-259

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTFR-2016-AVI-259
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	03 août 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2016-62 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-72 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-73 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-63 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-64 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-67 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-75 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-77 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-78 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-79 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-65 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-68 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-69 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-70 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-71 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-74 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-76 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-80 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-81 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-82 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-84 du 02 août 2016 Bulletin de sécurité Mozilla mfsa2016-83 du 02 août 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
- déni de service à distance

- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- Firefox versions antérieures à 48
- Firefox ESR versions antérieures à 45.3

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Mozilla Firefox*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Mozilla mfsa2016-62 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-62/
- Bulletin de sécurité Mozilla mfsa2016-72 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-72/
- Bulletin de sécurité Mozilla mfsa2016-73 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-73/
- Bulletin de sécurité Mozilla mfsa2016-63 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-63/
- Bulletin de sécurité Mozilla mfsa2016-64 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-64/
- Bulletin de sécurité Mozilla mfsa2016-67 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-67/
- Bulletin de sécurité Mozilla mfsa2016-75 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/
- Bulletin de sécurité Mozilla mfsa2016-77 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-77/
- Bulletin de sécurité Mozilla mfsa2016-78 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-78/
- Bulletin de sécurité Mozilla mfsa2016-79 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-79/
- Bulletin de sécurité Mozilla mfsa2016-65 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-65/
- Bulletin de sécurité Mozilla mfsa2016-68 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-68/
- Bulletin de sécurité Mozilla mfsa2016-69 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-69/
- Bulletin de sécurité Mozilla mfsa2016-70 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-70/
- Bulletin de sécurité Mozilla mfsa2016-71 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-71/

- Bulletin de sécurité Mozilla mfsa2016-74 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-74/
- Bulletin de sécurité Mozilla mfsa2016-76 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-76/
- Bulletin de sécurité Mozilla mfsa2016-80 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-80/
- Bulletin de sécurité Mozilla mfsa2016-81 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-81/
- Bulletin de sécurité Mozilla mfsa2016-82 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-82/
- Bulletin de sécurité Mozilla mfsa2016-84 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-84/
- Bulletin de sécurité Mozilla mfsa2016-83 du 02 août 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-83/
- Référence CVE CVE-2016-0718
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0718
- Référence CVE CVE-2016-2830
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2830
- Référence CVE CVE-2016-2836
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2836
- Référence CVE CVE-2016-2837
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2837
- Référence CVE CVE-2016-2838
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2838
- Référence CVE CVE-2016-2839
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2839
- Référence CVE CVE-2016-5250
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5250
- Référence CVE CVE-2016-5252
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5252
- Référence CVE CVE-2016-5253
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5253
- Référence CVE CVE-2016-5254
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5254
- Référence CVE CVE-2016-5255
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5255
- Référence CVE CVE-2016-5258
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5258
- Référence CVE CVE-2016-5259
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5259
- Référence CVE CVE-2016-5260
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5260
- Référence CVE CVE-2016-5261
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5261
- Référence CVE CVE-2016-5262
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5262
- Référence CVE CVE-2016-5263
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5263
- Référence CVE CVE-2016-5264
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5264
- Référence CVE CVE-2016-5265
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5265
- Référence CVE CVE-2016-5266
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5266

- Référence CVE CVE-2016-5267
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5267
- Référence CVE CVE-2016-5268
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5268

Gestion détaillée du document

03 août 2016 version initiale.