

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTFR-2016-AVI-193
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	08 juin 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2016-49 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-50 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-51 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-53 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-55 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-56 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-58 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-52 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-59 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-60 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-61 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-54 du 07 juin 2016 Bulletin de sécurité Mozilla mfsa2016-57 du 07 juin 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 la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Firefox versions antérieures à 47

- Firefox ESR versions antérieures à 45.2

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 mfsa2016-49 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-49/>
- Bulletin de sécurité Mozilla mfsa2016-50 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-50/>
- Bulletin de sécurité Mozilla mfsa2016-51 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-51/>
- Bulletin de sécurité Mozilla mfsa2016-53 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-53/>
- Bulletin de sécurité Mozilla mfsa2016-55 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-55/>
- Bulletin de sécurité Mozilla mfsa2016-56 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-56/>
- Bulletin de sécurité Mozilla mfsa2016-58 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-58/>
- Bulletin de sécurité Mozilla mfsa2016-52 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-52/>
- Bulletin de sécurité Mozilla mfsa2016-59 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-59/>
- Bulletin de sécurité Mozilla mfsa2016-60 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-60/>
- Bulletin de sécurité Mozilla mfsa2016-61 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-61/>
- Bulletin de sécurité Mozilla mfsa2016-54 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-54/>
- Bulletin de sécurité Mozilla mfsa2016-57 du 07 juin 2016
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-57/>
- Référence CVE CVE-2016-2818
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2818>
- Référence CVE CVE-2016-2815
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2815>
- Référence CVE CVE-2016-2819
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2819>
- Référence CVE CVE-2016-2821
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2821>
- Référence CVE CVE-2016-2824
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2824>
- Référence CVE CVE-2016-2826
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2826>
- Référence CVE CVE-2016-2828
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2828>

- Référence CVE CVE-2016-2831
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2831>
- Référence CVE CVE-2016-2822
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2822>
- Référence CVE CVE-2016-2832
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2832>
- Référence CVE CVE-2016-2833
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2833>
- Référence CVE CVE-2016-2834
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2834>
- Référence CVE CVE-2016-2825
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2825>
- Référence CVE CVE-2016-2829
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2829>

Gestion détaillée du document

08 juin 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-193>
