

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTFR-2015-AVI-461
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	04 novembre 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2015-133 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-132 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-131 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-130 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-129 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-128 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-127 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-126 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-125 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-124 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-123 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-122 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-121 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-120 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-119 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-118 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-117 du 03 novembre 2015 Bulletin de sécurité Mozilla mfsa2015-116 du 03 novembre 2015
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 code indirecte à distance

2 - Systèmes affectés

- Mozilla Firefox versions antérieures à 42
- Mozilla Firefox ESR versions antérieures à 38.4

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 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 Mozilla mfsa2015-133 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-133/>
- Bulletin de sécurité Mozilla mfsa2015-132 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-132/>
- Bulletin de sécurité Mozilla mfsa2015-131 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-131/>
- Bulletin de sécurité Mozilla mfsa2015-130 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-130/>
- Bulletin de sécurité Mozilla mfsa2015-129 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-129/>
- Bulletin de sécurité Mozilla mfsa2015-128 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-128/>
- Bulletin de sécurité Mozilla mfsa2015-127 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-127/>
- Bulletin de sécurité Mozilla mfsa2015-126 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-126/>
- Bulletin de sécurité Mozilla mfsa2015-125 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-125/>
- Bulletin de sécurité Mozilla mfsa2015-124 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-124/>
- Bulletin de sécurité Mozilla mfsa2015-123 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-123/>
- Bulletin de sécurité Mozilla mfsa2015-122 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-122/>
- Bulletin de sécurité Mozilla mfsa2015-121 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-121/>
- Bulletin de sécurité Mozilla mfsa2015-120 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-120/>
- Bulletin de sécurité Mozilla mfsa2015-119 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-119/>
- Bulletin de sécurité Mozilla mfsa2015-118 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-118/>
- Bulletin de sécurité Mozilla mfsa2015-117 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-117/>
- Bulletin de sécurité Mozilla mfsa2015-116 du 03 novembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-116/>

- Référence CVE CVE-2015-4513
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4513>
- Référence CVE CVE-2015-4514
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4514>
- Référence CVE CVE-2015-4515
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4515>
- Référence CVE CVE-2015-4518
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4518>
- Référence CVE CVE-2015-7186
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7186>
- Référence CVE CVE-2015-7187
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7187>
- Référence CVE CVE-2015-7188
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7188>
- Référence CVE CVE-2015-7189
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7189>
- Référence CVE CVE-2015-7190
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7190>
- Référence CVE CVE-2015-7191
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7191>
- Référence CVE CVE-2015-7192
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7192>
- Référence CVE CVE-2015-7193
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7193>
- Référence CVE CVE-2015-7194
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7194>
- Référence CVE CVE-2015-7195
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7195>
- Référence CVE CVE-2015-7196
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7196>
- Référence CVE CVE-2015-7198
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7198>
- Référence CVE CVE-2015-7199
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7199>
- Référence CVE CVE-2015-7200
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7200>
- Référence CVE CVE-2015-7197
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7197>
- Référence CVE CVE-2015-7181
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7181>
- Référence CVE CVE-2015-7182
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7182>
- Référence CVE CVE-2015-7183
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7183>
- Référence CVE CVE-2015-7185
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7185>

Gestion détaillée du document

04 novembre 2015 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-2015-AVI-461>
