

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Mozilla

Gestion du document

Référence	CERTFR-2015-AVI-543
Titre	Multiples vulnérabilités dans Mozilla
Date de la première version	16 décembre 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2015-134 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-135 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-136 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-137 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-138 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-139 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-140 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-141 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-142 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-143 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-144 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-145 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-146 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-147 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-148 du 15 décembre 2015 Bulletin de sécurité Mozilla mfsa2015-149 du 15 décembre 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
- 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
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Firefox versions antérieures à 43
- Firefox ESR versions antérieures à 38.5

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *Mozilla*. 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 mfsa2015-134 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-134/>
- Bulletin de sécurité Mozilla mfsa2015-135 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-135/>
- Bulletin de sécurité Mozilla mfsa2015-136 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-136/>
- Bulletin de sécurité Mozilla mfsa2015-137 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-137/>
- Bulletin de sécurité Mozilla mfsa2015-138 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-138/>
- Bulletin de sécurité Mozilla mfsa2015-139 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-139/>
- Bulletin de sécurité Mozilla mfsa2015-140 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-140/>
- Bulletin de sécurité Mozilla mfsa2015-141 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-141/>
- Bulletin de sécurité Mozilla mfsa2015-142 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-142/>
- Bulletin de sécurité Mozilla mfsa2015-143 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-143/>
- Bulletin de sécurité Mozilla mfsa2015-144 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-144/>
- Bulletin de sécurité Mozilla mfsa2015-145 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-145/>
- Bulletin de sécurité Mozilla mfsa2015-146 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-146/>
- Bulletin de sécurité Mozilla mfsa2015-147 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-147/>
- Bulletin de sécurité Mozilla mfsa2015-148 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-148/>
- Bulletin de sécurité Mozilla mfsa2015-149 du 15 décembre 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-149/>
- Référence CVE CVE-2015-7203
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7203>
- Référence CVE CVE-2015-7220
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7220>

- Référence CVE CVE-2015-7221
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7221>
- Référence CVE CVE-2015-7204
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7204>
- Référence CVE CVE-2015-7215
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7215>
- Référence CVE CVE-2015-7214
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7214>
- Référence CVE CVE-2015-7218
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7218>
- Référence CVE CVE-2015-7219
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7219>
- Référence CVE CVE-2015-7208
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7208>
- Référence CVE CVE-2015-7211
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7211>
- Référence CVE CVE-2015-7223
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7223>
- Référence CVE CVE-2015-7222
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7222>
- Référence CVE CVE-2015-7213
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7213>
- Référence CVE CVE-2015-7205
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7205>
- Référence CVE CVE-2015-7216
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7216>
- Référence CVE CVE-2015-7217
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7217>
- Référence CVE CVE-2015-7212
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7212>
- Référence CVE CVE-2015-7210
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7210>
- Référence CVE CVE-2015-7207
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7207>
- Référence CVE CVE-2015-7201
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7201>
- Référence CVE CVE-2015-7202
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7202>

Gestion détaillée du document

16 décembre 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-543>
