

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans les produits Mozilla

### Gestion du document

Référence	CERTFR-2015-AVI-020
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	14 janvier 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2015-01 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-02 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-03 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-04 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-05 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-06 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-07 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-08 du 13 janvier 2015 Bulletin de sécurité Mozilla mfsa2015-09 du 13 janvier 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
- élévation de privilèges
- injection de requêtes illégitimes par rebond

## 2 - Systèmes affectés

- Firefox versions antérieures à 35
- Firefox ESR versions antérieures à 31.4
- SeaMonkey versions antérieures à 2.32
- ThunderBird versions antérieures à 31.4

### 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 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 mfsa2015-01 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-01/>
- Bulletin de sécurité Mozilla mfsa2015-02 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-02/>
- Bulletin de sécurité Mozilla mfsa2015-03 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-03/>
- Bulletin de sécurité Mozilla mfsa2015-04 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-04/>
- Bulletin de sécurité Mozilla mfsa2015-05 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-05/>
- Bulletin de sécurité Mozilla mfsa2015-06 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-06/>
- Bulletin de sécurité Mozilla mfsa2015-07 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-07/>
- Bulletin de sécurité Mozilla mfsa2015-08 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-08/>
- Bulletin de sécurité Mozilla mfsa2015-09 du 13 janvier 2015  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-09/>
- Référence CVE CVE-2014-8634  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8634>
- Référence CVE CVE-2014-8635  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8635>
- Référence CVE CVE-2014-8636  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8636>
- Référence CVE CVE-2014-8637  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8637>
- Référence CVE CVE-2014-8638  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8638>
- Référence CVE CVE-2014-8639  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8639>
- Référence CVE CVE-2014-8640  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8640>
- Référence CVE CVE-2014-8641  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8641>
- Référence CVE CVE-2014-8642  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8642>
- Référence CVE CVE-2014-8643  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8643>

## Gestion détaillée du document

14 janvier 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-020>

---