

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans les produits Mozilla

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTFR-2014-AVI-503  |
| Titre                       | Multiples vulnérabilités dans les produits Mozilla   |
| Date de la première version | 02 décembre 2014   |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité Mozilla mfsa2014-83 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-84 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-85 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-86 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-87 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-88 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-89 du 02 décembre 2014<br>Bulletin de sécurité Mozilla mfsa2014-90 du 02 décembre 2014 |
| 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

## 2 - Systèmes affectés

- Versions antérieures à Firefox 34
- versions antérieures à Firefox ESR 31.3
- versions antérieures à Thunderbird 31.3

### 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 mfsa2014-83 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-83/>
- Bulletin de sécurité Mozilla mfsa2014-84 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-84/>
- Bulletin de sécurité Mozilla mfsa2014-85 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-85/>
- Bulletin de sécurité Mozilla mfsa2014-86 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-86/>
- Bulletin de sécurité Mozilla mfsa2014-87 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-87/>
- Bulletin de sécurité Mozilla mfsa2014-88 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-88/>
- Bulletin de sécurité Mozilla mfsa2014-89 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-89/>
- Bulletin de sécurité Mozilla mfsa2014-90 du 02 décembre 2014  
<https://www.mozilla.org/en-US/security/advisories/mfsa2014-90/>
- Référence CVE CVE-2014-1587  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1587>
- Référence CVE CVE-2014-1588  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1588>
- Référence CVE CVE-2014-1589  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1589>
- Référence CVE CVE-2014-1590  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1590>
- Référence CVE CVE-2014-1591  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1591>
- Référence CVE CVE-2014-1592  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1592>
- Référence CVE CVE-2014-1593  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1593>
- Référence CVE CVE-2014-1594  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1594>
- Référence CVE CVE-2014-1595  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1595>

## Gestion détaillée du document

**02 décembre 2014** version initiale.