

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTFR-2015-AVI-131
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	01 avril 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2015-30 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-31 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-32 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-33 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-34 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-35 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-36 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-37 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-38 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-39 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-40 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-41 du 31 mars 2015 Bulletin de sécurité Mozilla mfsa2015-42 du 31 mars 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 la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Mozilla Firefox versions antérieures à 37
- Mozilla Firefox ESR versions antérieures à 31.6
- Mozilla Thunderbird versions antérieures à 31.6

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 mfsa2015-30 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-30/>
- Bulletin de sécurité Mozilla mfsa2015-31 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-31/>
- Bulletin de sécurité Mozilla mfsa2015-32 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-32/>
- Bulletin de sécurité Mozilla mfsa2015-33 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-33/>
- Bulletin de sécurité Mozilla mfsa2015-34 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-34/>
- Bulletin de sécurité Mozilla mfsa2015-35 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-35/>
- Bulletin de sécurité Mozilla mfsa2015-36 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-36/>
- Bulletin de sécurité Mozilla mfsa2015-37 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-37/>
- Bulletin de sécurité Mozilla mfsa2015-38 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-38/>
- Bulletin de sécurité Mozilla mfsa2015-39 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-39/>
- Bulletin de sécurité Mozilla mfsa2015-40 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-40/>
- Bulletin de sécurité Mozilla mfsa2015-41 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-41/>
- Bulletin de sécurité Mozilla mfsa2015-42 du 31 mars 2015
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-42/>
- Référence CVE CVE-2015-0814
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0814>
- Référence CVE CVE-2015-0815
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0815>
- Référence CVE CVE-2015-0813
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0813>
- Référence CVE CVE-2015-0812
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0812>
- Référence CVE CVE-2015-0816
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0816>

- Référence CVE CVE-2015-0811
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0811>
- Référence CVE CVE-2015-0810
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0810>
- Référence CVE CVE-2015-0808
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0808>
- Référence CVE CVE-2015-0807
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0807>
- Référence CVE CVE-2015-0805
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0805>
- Référence CVE CVE-2015-0806
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0806>
- Référence CVE CVE-2015-0803
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0803>
- Référence CVE CVE-2015-0804
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0804>
- Référence CVE CVE-2015-0801
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0801>
- Référence CVE CVE-2015-0800
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0800>
- Référence CVE CVE-2012-2808
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2808>
- Référence CVE CVE-2015-0802
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0802>

Gestion détaillée du document

01 avril 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-131>
