Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 25 février 2015
N° CERTFR-2015-AVI-079

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTFR-2015-AVI-079
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	25 février 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2015-17 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-16 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-15 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-14 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-13 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-12 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-11 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-27 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-26 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-25 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-24 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-23 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-22 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-21 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-20 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-19 du 24 février 2015 Bulletin de sécurité Mozilla mfsa2015-18 du 24 février 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

2 - Systèmes affectés

- Mozilla Firefox versions antérieures à 36
- Mozilla Firefox ESR versions antérieures à 31.5
- Mozilla Thunderbird versions antérieures à 31.5

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 mfsa2015-17 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-17/
- Bulletin de sécurité Mozilla mfsa2015-16 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-16/
- Bulletin de sécurité Mozilla mfsa2015-15 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-15/
- Bulletin de sécurité Mozilla mfsa2015-14 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-14/
- Bulletin de sécurité Mozilla mfsa2015-13 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-13/
- Bulletin de sécurité Mozilla mfsa2015-12 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-12/
- Bulletin de sécurité Mozilla mfsa2015-11 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-11/
- Bulletin de sécurité Mozilla mfsa2015-27 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-27/
- Bulletin de sécurité Mozilla mfsa2015-26 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-26/
- Bulletin de sécurité Mozilla mfsa2015-25 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-25/
- Bulletin de sécurité Mozilla mfsa2015-24 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-24/
- Bulletin de sécurité Mozilla mfsa2015-23 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-23/
- Bulletin de sécurité Mozilla mfsa2015-22 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-22/
- Bulletin de sécurité Mozilla mfsa2015-21 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-21/
- Bulletin de sécurité Mozilla mfsa2015-20 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-20/
- Bulletin de sécurité Mozilla mfsa2015-19 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-19/
- Bulletin de sécurité Mozilla mfsa2015-18 du 24 février 2015
  https://www.mozilla.org/en-US/security/advisories/mfsa2015-18/
- Référence CVE CVE-2015-0829
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0829

- Référence CVE CVE-2015-0831
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0831
- Référence CVE CVE-2015-0834
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0834
- Référence CVE CVE-2015-0830
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0830
- Référence CVE CVE-2015-0832
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0832
- Référence CVE CVE-2015-0833
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0833
- Référence CVE CVE-2015-0835
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0835
- Référence CVE CVE-2015-0836
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0836
- Référence CVE CVE-2015-0820
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0820
- Référence CVE CVE-2015-0819
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0819
- Référence CVE CVE-2015-0821
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0821
- Référence CVE CVE-2015-0822
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0822
- Référence CVE CVE-2015-0823
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0823
- Référence CVE CVE-2015-0824
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0824
- Référence CVE CVE-2015-0825
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0825
- Référence CVE CVE-2015-0826
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0826
- Référence CVE CVE-2015-0827
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0827
- Référence CVE CVE-2015-0828
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0828

Gestion détaillée du document

25 février 2015 version initiale.