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 08 mars 2016
N° CERTFR-2016-AVI-086

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTFR-2016-AVI-086
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	08 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2016-16 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-37 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-35 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-22 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-23 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-24 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-27 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-25 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-36 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-17 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-34 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-29 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-33 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-31 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-30 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-15 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-18 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-19 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-21 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-26 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-28 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-32 du 08 mars 2016 Bulletin de sécurité Mozilla mfsa2016-20 du 08 mars 2016
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

2 - Systèmes affectés

- Firefox versions antérieures à 45
- Firefox ESR versions antérieures à 38.7
- NSS versions antérieures à 3.21.1
- NSS versions antérieures à 3.19.2.3

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Mozilla Firefox*. 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 mfsa2016-16 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-16/
- Bulletin de sécurité Mozilla mfsa2016-37 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-37/
- Bulletin de sécurité Mozilla mfsa2016-35 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-35/
- Bulletin de sécurité Mozilla mfsa2016-22 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-22/
- Bulletin de sécurité Mozilla mfsa2016-23 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-23/
- Bulletin de sécurité Mozilla mfsa2016-24 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-24/
- Bulletin de sécurité Mozilla mfsa2016-27 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-27/
- Bulletin de sécurité Mozilla mfsa2016-25 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-25/
- Bulletin de sécurité Mozilla mfsa2016-36 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-36/
- Bulletin de sécurité Mozilla mfsa2016-17 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-17/
- Bulletin de sécurité Mozilla mfsa2016-34 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-34/
- Bulletin de sécurité Mozilla mfsa2016-29 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-29/
- Bulletin de sécurité Mozilla mfsa2016-33 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-33/
- Bulletin de sécurité Mozilla mfsa2016-31 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-31/

- Bulletin de sécurité Mozilla mfsa2016-30 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-30/
- Bulletin de sécurité Mozilla mfsa2016-15 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-15/
- Bulletin de sécurité Mozilla mfsa2016-18 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-18/
- Bulletin de sécurité Mozilla mfsa2016-19 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-19/
- Bulletin de sécurité Mozilla mfsa2016-21 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-21/
- Bulletin de sécurité Mozilla mfsa2016-26 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-26/
- Bulletin de sécurité Mozilla mfsa2016-28 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-28/
- Bulletin de sécurité Mozilla mfsa2016-32 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-32/
- Bulletin de sécurité Mozilla mfsa2016-20 du 08 mars 2016
  https://www.mozilla.org/en-US/security/advisories/mfsa2016-20/
- Référence CVE CVE-2016-1950
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1950
- Référence CVE CVE-2016-1952
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1952
- Référence CVE CVE-2016-1953
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1953
- Référence CVE CVE-2016-1954
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1954
- Référence CVE CVE-2016-1955
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1955
- Référence CVE CVE-2016-1956
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1956
- Référence CVE CVE-2016-1957
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1957
- Référence CVE CVE-2016-1958
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1958
- Référence CVE CVE-2016-1959
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1959
- Référence CVE CVE-2016-1960
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1960
- Référence CVE CVE-2016-1961
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1961
- Référence CVE CVE-2016-1962
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1962
- Référence CVE CVE-2016-1963
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1963
- Référence CVE CVE-2016-1964
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1964
- Référence CVE CVE-2016-1965
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1965
- Référence CVE CVE-2016-1966
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1966
- Référence CVE CVE-2016-1967
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1967
- Référence CVE CVE-2016-1968
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1968

- Référence CVE CVE-2016-1970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1970
- Référence CVE CVE-2016-1971
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1971
- Référence CVE CVE-2016-1972
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1972
- Référence CVE CVE-2016-1973
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1973
- Référence CVE CVE-2016-1974
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1974
- Référence CVE CVE-2016-1975
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1975
- Référence CVE CVE-2016-1976
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1976
- Référence CVE CVE-2016-1977
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1977
- Référence CVE CVE-2016-1978
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1978
- Référence CVE CVE-2016-1979
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1979
- Référence CVE CVE-2016-2790
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2790
- Référence CVE CVE-2016-2791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2791
- Référence CVE CVE-2016-2792
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2792
- Référence CVE CVE-2016-2793
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2793
- Référence CVE CVE-2016-2794
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2794
- Référence CVE CVE-2016-2795
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2795
- Référence CVE CVE-2016-2796
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2796
- Référence CVE CVE-2016-2797
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2797
- Référence CVE CVE-2016-2798
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2798
- Référence CVE CVE-2016-2799
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2799
- Référence CVE CVE-2016-2800
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2800
- Référence CVE CVE-2016-2801
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2801
- Référence CVE CVE-2016-2802
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2802

Gestion détaillée du document

08 mars 2016 version initiale.