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 03 juillet 2015
N° CERTFR-2015-AVI-279

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTFR-2015-AVI-279
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	03 juillet 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla MFSA 2015-59 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-60 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-61 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-62 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-63 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-64 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-65 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-66 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-67 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-68 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-69 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-70 du 02 juillet 2015 Bulletin de sécurité Mozilla MFSA 2015-71 du 02 juillet 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
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Librairie NSS versions antérieures à 3.19.1
- Mozilla Firefox versions antérieures à 39
- Mozilla Firefox ESR versions antérieures à 31.8

– Mozilla Firefox ESR versions antérieures à 38.1
– Mozilla Thunderbird versions antérieures à 38.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Mozilla*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges.

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 MFSA 2015-59 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-59/
– Bulletin de sécurité Mozilla MFSA 2015-60 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-60/
– Bulletin de sécurité Mozilla MFSA 2015-61 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-61
– Bulletin de sécurité Mozilla MFSA 2015-62 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-62
– Bulletin de sécurité Mozilla MFSA 2015-63 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-63
– Bulletin de sécurité Mozilla MFSA 2015-64 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-64
– Bulletin de sécurité Mozilla MFSA 2015-65 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-65
– Bulletin de sécurité Mozilla MFSA 2015-66 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-66
– Bulletin de sécurité Mozilla MFSA 2015-67 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-67
– Bulletin de sécurité Mozilla MFSA 2015-68 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-68
– Bulletin de sécurité Mozilla MFSA 2015-69 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-69
– Bulletin de sécurité Mozilla MFSA 2015-70 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-70
– Bulletin de sécurité Mozilla MFSA 2015-71 du 02 juillet 2015
https://www.mozilla.org/en-US/security/advisories/mfsa2015-71
– Référence CVE CVE-2015-2721
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2721
– Référence CVE CVE-2015-4000
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
– Référence CVE CVE-2015-2743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2743
– Référence CVE CVE-2015-2742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2742
– Référence CVE CVE-2015-2741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2741
– Référence CVE CVE-2015-2734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2734

- Référence CVE CVE-2015-2735
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2735
- Référence CVE CVE-2015-2736
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2736
- Référence CVE CVE-2015-2737
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2737
- Référence CVE CVE-2015-2738
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2738
- Référence CVE CVE-2015-2739
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2739
- Référence CVE CVE-2015-2740
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2740
- Référence CVE CVE-2015-2722
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2722
- Référence CVE CVE-2015-2733
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2733
- Référence CVE CVE-2015-2730
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2730
- Référence CVE CVE-2015-2729
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2729
- Référence CVE CVE-2015-2728
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2728
- Référence CVE CVE-2015-2727
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2727
- Référence CVE CVE-2015-2724
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2724
- Référence CVE CVE-2015-2725
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2725
- Référence CVE CVE-2015-2726
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2726

Gestion détaillée du document

03 juillet 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-279`