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 30 avril 2014
N° CERTFR-2014-AVI-209

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTFR-2014-AVI-209
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	30 avril 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2014-34 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-35 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-36 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-37 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-38 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-39 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-40 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-41 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-42 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-43 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-44 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-45 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-46 du 29 avril 2014 Bulletin de sécurité Mozilla mfsa2014-47 du 29 avril 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
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Versions antérieures à Firefox 29

- versions antérieures à Firefox ESR 24.5
- versions antérieures à Thunderbird 24.5
- versions antérieures à Seamonkey 2.26

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 mfsa2014-34 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-34.html
- Bulletin de sécurité Mozilla mfsa2014-35 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-35.html
- Bulletin de sécurité Mozilla mfsa2014-36 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-36.html
- Bulletin de sécurité Mozilla mfsa2014-37 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-37.html
- Bulletin de sécurité Mozilla mfsa2014-38 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-38.html
- Bulletin de sécurité Mozilla mfsa2014-39 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-39.html
- Bulletin de sécurité Mozilla mfsa2014-40 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-40.html
- Bulletin de sécurité Mozilla mfsa2014-41 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-41.html
- Bulletin de sécurité Mozilla mfsa2014-42 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-42.html
- Bulletin de sécurité Mozilla mfsa2014-43 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-43.html
- Bulletin de sécurité Mozilla mfsa2014-44 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-44.html
- Bulletin de sécurité Mozilla mfsa2014-45 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-45.html
- Bulletin de sécurité Mozilla mfsa2014-46 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-46.html
- Bulletin de sécurité Mozilla mfsa2014-47 du 29 avril 2014
  http://www.mozilla.org/security/announce/2014/mfsa2014-47.html
- Référence CVE CVE-2014-1492
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1492
- Référence CVE CVE-2014-1518
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1518
- Référence CVE CVE-2014-1519
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1519
- Référence CVE CVE-2014-1520
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1520
- Référence CVE CVE-2014-1522
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1522

- Référence CVE CVE-2014-1523
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1523
- Référence CVE CVE-2014-1524
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1524
- Référence CVE CVE-2014-1525
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1525
- Référence CVE CVE-2014-1526
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1526
- Référence CVE CVE-2014-1527
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1527
- Référence CVE CVE-2014-1528
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1528
- Référence CVE CVE-2014-1529
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1529
- Référence CVE CVE-2014-1530
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1530
- Référence CVE CVE-2014-1531
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1531
- Référence CVE CVE-2014-1532
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1532

Gestion détaillée du document

30 avril 2014 version initiale.