Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 06 juin 2012
N° CERTA-2012-AVI-307

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTA-2012-AVI-307
Titre	Vulnérabilités dans les produits Mozilla
Date de la première version	06 juin 2012
Date de la dernière version	–
Source(s)	Bulletins Mozilla mfsa2012 du 05 juin 2012
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Firefox versions antérieures à 13.0 ;
- Firefox ESR versions antérieures à 10.0.5 ;
- Thunderbird versions antérieures à 13.0 ;
- Thunderbird ESR versions antérieures à 10.0.5 ;
- SeaMonkey versions antérieures à 2.10.

3 Résumé

Plusieurs vulnérabilités ont été corrigées pour les produits Mozilla. Leur exploitation permet notamment l'exécution de code arbitraire à distance.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-34 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-34.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-35 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-35.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-36 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-36.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-37 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-37.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-38 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-38.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-39 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-39.html
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-40 du 05 juin 2012 : http://www.mozilla.org/security/announce/2012/mfsa2012-40.html
- Référence CVE CVE-2011-3101 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3101
- Référence CVE CVE-2012-0441 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0441
- Référence CVE CVE-2012-1937 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1937
- Référence CVE CVE-2012-1938 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1938
- Référence CVE CVE-2012-1939 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1939
- Référence CVE CVE-2012-1940 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1940
- Référence CVE CVE-2012-1941 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1941
- Référence CVE CVE-2012-1942 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1942
- Référence CVE CVE-2012-1943 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1943
- Référence CVE CVE-2012-1944 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1944
- Référence CVE CVE-2012-1945 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1945
- Référence CVE CVE-2012-1946 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1946
- Référence CVE CVE-2012-1947 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1947

Gestion détaillée du document

06 juin 2012 version initiale.