

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Mozilla

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-047>

Gestion du document

Référence	CERTA-2012-AVI-047
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	01 février 2012
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla du 31 janvier 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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Firefox versions antérieures à 10.0 ;
- Firefox versions antérieures à 3.6.26 ;
- Thunderbird versions antérieures à 10.0 ;
- Thunderbird versions antérieures à 3.1.18 ;
- Seamonkey versions antérieures à 2.7.

3 Résumé

Plusieurs vulnérabilités corrigées dans les produits Mozilla peuvent être exploitées pour contourner la politique de sécurité, injecter du code indirectement à distance, ou exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été corrigées dans les produits de la gamme Mozilla :

- plusieurs problèmes de corruption mémoire peuvent être exploités pour exécuter du code arbitraire à distance (CVE-2012-0442, 443 et 449) ;
- un problème dans l'interprétation des adresses réticulaires peut être exploité dans certaines circonstances pour divulguer des informations sur la navigation (CVE-2011-3670) ;
- un problème dans la gestion des noms de fenêtre peut être exploité pour remplacer des fenêtres par d'autres (CVE-2012-0445) ;
- un problème d'utilisation d'un pointeur après sa libération peut être exploité pour exécuter du code arbitraire à distance (CVE-2011-3659) ;
- un manquement dans le contrôle de sécurité entre les fenêtres peut être exploité pour une injection de code indirecte à distance (CVE-2012-0446) ;
- un problème dans la gestion des tailles d'icône peut être exploité pour contourner la politique de sécurité (CVE-2012-0447) ;
- un problème de corruption mémoire lors de la lecture de fichiers Ogg Vorbis peut être exploité pour exécuter du code arbitraire à distance (CVE-2012-0444) ;
- un problème de droits lors de l'exportation de la clef Firefox Sync sur les systèmes Linux et MacOS peut être exploité pour contourner la politique de sécurité (CVE-2012-0450).

5 Solution

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

6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-01 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-01.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-02 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-02.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-03 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-03.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-04 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-04.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-05 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-05.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-06 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-06.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-07 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-07.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-08 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-08.html>
- Bulletin de sécurité de la fondation Mozilla 2012/mfsa2012-09 du 31 janvier 2012 : <http://www.mozilla.org/security/announce/2012/mfsa2012-09.html>
- Référence CVE CVE-2012-0442 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0442>
- Référence CVE CVE-2012-0443 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0443>
- Référence CVE CVE-2012-0444 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0444>
- Référence CVE CVE-2012-0445 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0445>
- Référence CVE CVE-2012-0446 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0446>

- Référence CVE CVE-2012-0447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0447>
- Référence CVE CVE-2012-0449 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0449>
- Référence CVE CVE-2012-0450 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0450>
- Référence CVE CVE-2011-3659 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3659>
- Référence CVE CVE-2011-3670 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3670>

Gestion détaillée du document

01 février 2012 version initiale.