

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-2011-AVI-365>

Gestion du document

Référence	CERTA-2011-AVI-365
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	22 juin 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla mfsa2011-19 à mfsa2011-28 du 21 juin 2011
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 ;

2 Systèmes affectés

- Mozilla Firefox versions 3.x antérieures à la version 3.6.18 ;
- Mozilla Firefox 4.x (toutes versions) ;
- Mozilla Thunderbird versions 3.x inférieures à la version 3.1.11.

3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits Mozilla, dont certaines permettent l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été corrigées dans les produits Mozilla dont :

- Plusieurs vulnérabilités dans la gestion de la mémoire de Firefox et Thunderbird permettent à un utilisateur malintentionné d'exécuter du code arbitraire à distance ;
- plusieurs vulnérabilités dans WebGL (Firefox 4.x uniquement) permettent à un utilisateur malintentionné d'exécuter du code arbitraire à distance ou de contourner la politique de sécurité «*same-origin policy*» ;
- une vulnérabilité dans le traitement des documents XUL permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

5 Solution

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

Note : les utilisateurs de la version 4.x de Firefox doivent migrer vers la version 5.0 afin d'appliquer les correctifs.

6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-19 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-19.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-20 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-20.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-21 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-21.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-22 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-22.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-23 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-23.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-24 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-24.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-25 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-25.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-26 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-26.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-27 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-27.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-28 du 21 juin 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-28.html>
- Référence CVE CVE-2011-0083 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0083>
- Référence CVE CVE-2011-0085 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0085>
- Référence CVE CVE-2011-2362 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2362>
- Référence CVE CVE-2011-2363 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2363>
- Référence CVE CVE-2011-2364 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2364>
- Référence CVE CVE-2011-2365 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2365>
- Référence CVE CVE-2011-2366 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2366>

- Référence CVE CVE-2011-2367 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2367>
- Référence CVE CVE-2011-2368 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2368>
- Référence CVE CVE-2011-2369 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2369>
- Référence CVE CVE-2011-2370 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2370>
- Référence CVE CVE-2011-2371 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2371>
- Référence CVE CVE-2011-2373 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2373>
- Référence CVE CVE-2011-2374 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2374>
- Référence CVE CVE-2011-2375 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2375>
- Référence CVE CVE-2011-2376 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2376>
- Référence CVE CVE-2011-2377 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2377>

Gestion détaillée du document

22 juin 2011 version initiale.