

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2010-AVI-585>

Gestion du document

Référence	CERTA-2010-AVI-585-001
Titre	Vulnérabilités dans les produits Mozilla
Date de la première version	10 décembre 2010
Date de la dernière version	24 décembre 2010
Source(s)	Bulletins de sécurité de la fondation Mozilla MFSA2010-74 à MFSA2010-84
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 ;
- déni de service à distance ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Firefox 3.5.x et 3.6.x ;
- Thunderbird 3.0.x et 3.1.x ;
- Seamonkey 2.0.x.

3 Résumé

Plusieurs vulnérabilités sont présentes dans les produits Mozilla et certaines permettent à un utilisateur malveillant d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Plusieurs vulnérabilités présentes dans les produits Mozilla ont été corrigées :

- des erreurs dans le moteur du navigateur provoquent des corruptions de la mémoire. Certaines permettraient d'exécuter du code arbitraire ;
- sur les plateformes Windows, un débordement de mémoire quand *document.write* est appelé permet de provoquer un arrêt inopiné ou d'exécuter du code arbitraire ;
- l'utilisation de *windows.open* dans certaines conditions permet d'utiliser les droits de *chrome* ;
- des objets HTML dans un arbre XUL sont utilisables pour provoquer un arrêt inopiné ou pour exécuter du code arbitraire ;
- des vulnérabilités sont exploitables au moyen de fontes de caractères ;
- le script Java *LiveConnect* permet, dans certaines circonstances, de contourner la politique de sécurité ;
- des utilisations de pointeurs après libération de la mémoire correspondante existent ;
- des tableaux JavaScript permettent de corrompre la mémoire ;
- les programmes en Javascript peuvent être exécutés avec des privilèges non prévus ;
- les pages d'erreurs réseau ou liées aux certificats peuvent être utilisées par des sites malveillants pour tromper l'utilisateur sur l'identité du site avec lequel il pense être connecté ;
- des jeux de caractères, hébreu, farsi et arabe, permettent de réaliser des injections de code indirectes.

5 Solution

Les versions 3.6.13 et 3.5.16 de Firefox, 3.1.7 et 3.0.11 de Thunderbird et 2.0.11 de SeaMonkey remédient à ces problèmes.

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

6 Documentation

- Bulletins de sécurité de la fondation Mozilla MFSA2010-74 à MFSA2010-84 du 09 décembre 2010 :
<http://www.mozilla.org/security/announce/2010/mfsa2010-74.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-75.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-76.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-77.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-78.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-79.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-80.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-81.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-82.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-83.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-84.html>
- Bulletins de sécurité Fedora FEDORA-2010-18777 et FEDORA-2010-18778 du 09 décembre 2010 (Mozilla Thunderbird) :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052110.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052220.html>
- Bulletins de sécurité Fedora FEDORA-2010-18890 et FEDORA-2010-18920 du 15 décembre 2010 (Mozilla Seamonkey) :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052502.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052504.html>
- Bulletins de sécurité Fedora FEDORA-2010-18773 et FEDORA-2010-18775 du 09 décembre 2010 (Mozilla Firefox) :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052029.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052035.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052023.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/052021.html>

- Référence CVE CVE-2010-3766 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3766>
- Référence CVE CVE-2010-3767 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3767>
- Référence CVE CVE-2010-3768 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3768>
- Référence CVE CVE-2010-3769 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3769>
- Référence CVE CVE-2010-3770 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3770>
- Référence CVE CVE-2010-3771 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3771>
- Référence CVE CVE-2010-3772 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3772>
- Référence CVE CVE-2010-3773 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3773>
- Référence CVE CVE-2010-3774 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3774>
- Référence CVE CVE-2010-3775 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3775>
- Référence CVE CVE-2010-3776 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3776>
- Référence CVE CVE-2010-3777 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3777>
- Référence CVE CVE-2010-3778 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3778>

Gestion détaillée du document

10 décembre 2010 version initiale.

24 décembre 2010 ajout des références aux bulletins Fedora.