

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2005-AVI-095>

Gestion du document

Référence	CERTA-2005-AVI-095-004
Titre	Multiples vulnérabilités dans Mozilla
Date de la première version	02 mars 2005
Date de la dernière version	21 mars 2005
Source(s)	Bulletins de sécurité Mozilla
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Mozilla 1.7.x et versions antérieures ;
- Firefox 1.x et versions antérieures ;
- Thunderbird 1.x et versions antérieures.

3 Résumé

De multiples vulnérabilités découvertes dans les applications basées sur le moteur Mozilla permettent à un utilisateur local ou distant mal intentionné d'exécuter de nombreuses actions malveillantes sur le système vulnérable.

4 Description

- Une vulnérabilité présente dans la création des fichiers temporaires permet à un utilisateur mal intentionné d'écraser des fichiers arbitraires via le suivi des liens symboliques (cf. MFSA 2005-28) ;
- une vulnérabilité liée à la présentation de l'invite d'authentification HTTP permet à un individu malveillant de porter atteinte à la confidentialité des données (cf. MFSA 2005-24) ;
- une vulnérabilité dans la fonction "enregistrer le lien sous ..." permet à un utilisateur mal intentionné, au moyen d'un site web malicieusement construit, de dissimuler l'extension du fichier à sauvegarder, à condition que l'option "cacher les extensions de type connues" soit activée sous Windows (cf. MFSA 2005-22) ;
- une vulnérabilité due à un mauvais traitement des fichiers raccourcis (.lnk) peut être exploitée afin de porter atteinte à l'intégrité des données présentes sur le système (cf. MFSA 2005-21) ;
- une vulnérabilité présente dans les documents XML (eXtended Markup Language) utilisant des feuilles de style de type XSLT (eXtended Styles Language Transformation) peut être exploitée afin de porter atteinte à la confidentialité des données (cf. MFSA 2005-20) ;
- une vulnérabilité présente dans la fonction qui permet de remplir automatiquement les champs de formulaires peut être exploitée pour porter atteinte à la confidentialité des données (cf. MFSA 2005-19) ;
- une vulnérabilité due à une erreur présente dans la bibliothèque de traitement des chaînes de caractères, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance (cf. MFSA 2005-18) ;
- un individu mal intentionné peut exploiter une vulnérabilité pour inciter l'utilisateur à installer des applications à partir de sites qui ne sont pas de confiance (cf. MFSA 2005-17) ;
- une vulnérabilité de type débordement de mémoire lors de la conversion de texte UTF8 en Unicode permet à une personne malveillante d'exécuter à distance du code arbitraire sur le système vulnérable (cf. MFSA 2005-15) ;
- une vulnérabilité pouvant être exploitée de plusieurs façons permet à un utilisateur mal intentionné de duper sa victime en lui faisant croire qu'elle accède à un site sécurisé (cf. MFSA 2005-14).

5 Solution

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

6 Documentation

- Site Internet de l'éditeur Mozilla :
<http://www.mozilla.org/>
- Mise à jour Firefox 1.0.1 :
<http://www.mozilla.org/products/firefox>
- Bulletin de sécurité Mozilla MFSA 2005-28 :
<http://www.mozilla.org/security/announce/mfsa2005-28.html>
- Bulletin de sécurité Mozilla MFSA 2005-24 :
<http://www.mozilla.org/security/announce/mfsa2005-24.html>
- Bulletin de sécurité Mozilla MFSA 2005-22 :
<http://www.mozilla.org/security/announce/mfsa2005-22.html>
- Bulletin de sécurité Mozilla MFSA 2005-21 :
<http://www.mozilla.org/security/announce/mfsa2005-21.html>
- Bulletin de sécurité Mozilla MFSA 2005-20 :
<http://www.mozilla.org/security/announce/mfsa2005-20.html>
- Bulletin de sécurité Mozilla MFSA 2005-19 :
<http://www.mozilla.org/security/announce/mfsa2005-19.html>
- Bulletin de sécurité Mozilla MFSA 2005-18 :
<http://www.mozilla.org/security/announce/mfsa2005-18.html>
- Bulletin de sécurité 200 d'iDefense du 28 février 2005 :
<http://www.iddefense.com/application/poi/display?id=200&type=vulnerabilities>
- Bulletin de sécurité Mozilla MFSA 2005-17 :
<http://www.mozilla.org/security/announce/mfsa2005-17.html>

- Bulletin de sécurité Mozilla MFSA 2005-15 :
<http://www.mozilla.org/security/announce/mfsa2005-15.html>
- Bulletin de sécurité Mozilla MFSA 2005-14 :
<http://www.mozilla.org/security/announce/mfsa2005-14.html>
- Bulletin de sécurité Gentoo GLSA 200503-10 / Firefox du 04 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml>
- Bulletin de sécurité RedHat RHSA-2005:277-10 du 04 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-277.html>
- Bulletin de sécurité RedHat RHSA-2005:176-11 du 1er mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-176.html>
- Mise à jour de sécurité des paquetages NetBSD firefox, firefox-bin, firefox-gtk2-bin :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/firefox/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/firefox-bin/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/firefox-bin-gtk2/README.html>
- Mise à jour de sécurité des paquetages NetBSD mozilla, mozilla-bin, mozilla-gtk2-bin :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/mozilla/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/mozilla-bin/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/mozilla-bin-gtk2/README.html>
- Bulletin de sécurité SUSE-SA:2005:016 du 16 mars 2005 :
http://www.novell.com/linux/security/advisories/2005_16_mozilla_firefox.html
- Référence CVE CAN-2005-0255 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0255>

Gestion détaillée du document

02 mars 2005 version initiale.

07 mars 2005 ajout de la référence au bulletin de sécurité RedHat.

08 mars 2005 ajout des références aux bulletins de sécurité RedHat et Gentoo.

09 mars 2005 ajout des références aux bulletins de sécurité NetBSD.

21 mars 2005 ajout de la référence au bulletin de sécurité SUSE.