

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-2006-AVI-391>

Gestion du document

Référence	CERTA-2006-AVI-391-002
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	14 septembre 2006
Date de la dernière version	28 septembre 2006
Source(s)	Mises à jour Mozilla du 14 septembre 2006
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Mozilla Firefox 1.5.0.6 ainsi que les versions antérieures ;
- Mozilla Thunderbird 1.5.0.5 ainsi que les versions antérieures ;
- Mozilla SeaMonkey 1.0.4 ainsi que les versions antérieures.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les produits Mozilla Firefox, Thunderbird et SeaMonkey. L'exploitation de ceux-ci contre un système vulnérable peuvent conduire à une exécution de code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les produits Mozilla Firefox, Thunderbird et SeaMonkey. Parmi celles-ci :

- la manipulation de certains codes `Javascript` par le navigateur Firefox pourrait provoquer un débordement de la mémoire, et ainsi permettre l'exécution de commandes arbitraires. L'utilisateur doit visiter une page construite de manière malveillante pour être impacté. Cependant, la messagerie Thunderbird utilise en grande partie le noyau du navigateur Firefox pour l'affichage de messages en format HTML, quand cela est autorisé. L'utilisateur pourrait donc avoir son système compromis suite à la lecture d'un courrier électronique. Cette option n'est pas activée par défaut.
- la désactivation de Javascript dans la messagerie Thunderbird ne serait pas correctement effectuée, et pourrait être contournée afin de permettre l'exécution de code Javascript à l'insu de l'utilisateur.
- une mauvaise vérification des signatures RSA PKCS #1 v1.5 utilisant un exposant de valeur 3. Cette vulnérabilité est à mettre en relation avec l'avis du CERTA CERTA-200-AVI-384 concernant OpenSSL.
- la procédure de mise à jour de Firefox et Thunderbird, basée sur SSL ne s'effectuerait pas correctement. Il serait possible, en usurpant les réponses DNS adressées à la victime, de rediriger ses requêtes de mises à jour vers un site malveillant. Le certificat ne serait alors pas convenablement vérifié.

5 Solution

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

6 Documentation

- Bulletin de sécurité SuSE SUSE-SA:2006:054 du 22 septembre 2006 :
<http://lists.suse.com/archive/suse-security-announce/2006-Sep/0008.html>
- Bulletin de sécurité Ubuntu USN-350 du 21 septembre 2006 :
<http://www.ubuntu.com/usn/usn-350-1>
- Bulletin de sécurité Ubuntu USN-351 du 22 septembre 2006 :
<http://www.ubuntu.com/usn/usn-351-1>
- Bulletin de sécurité Ubuntu USN-352 du 25 septembre 2006 :
<http://www.ubuntu.com/usn/usn-352-1>
- Bulletin de sécurité Mandriva MDKSA-2006:168 du 20 septembre 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:168>
- Bulletin de sécurité SGI 20060901-01-P du 19 septembre 2006 :
<ftp://patches.sgi.com/support/free/security/advisories/20060901-01-P.asc>
- Bulletin de sécurité Red Hat RHSA-2006:0675 du 15 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0675.html>
- Bulletin de sécurité Red Hat RHSA-2006:0676 du 15 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0676.html>
- Bulletin de sécurité Red Hat RHSA-2006:0677 du 15 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0677.html>
- Bulletin de sécurité Mozilla MFSA-2006-57 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-57.html>
- Bulletin de sécurité Mozilla MFSA-2006-58 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-58.html>
- Bulletin de sécurité Mozilla MFSA-2006-59 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-59.html>
- Bulletin de sécurité Mozilla MFSA-2006-60 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-60.html>
- Bulletin de sécurité Mozilla MFSA-2006-61 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-61.html>
- Bulletin de sécurité Mozilla MFSA-2006-62 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-62.html>

- Bulletin de sécurité Mozilla MFSA-2006-63 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-63.html>
- Bulletin de sécurité Mozilla MFSA-2006-64 :
<http://www.mozilla.org/security/announce/2006/mfsa2006-64.html>
- Référence CVE CVE-2006-4571 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4571>
- Référence CVE CVE-2006-4569 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4569>
- Référence CVE CVE-2006-4568 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4568>
- Référence CVE CVE-2006-4340 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4340>
- Référence CVE CVE-2006-4339 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339>
- Référence CVE CVE-2006-4253 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4253>
- Référence CVE CVE-2006-4567 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4567>
- Référence CVE CVE-2006-4565 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4565>
- Référence CVE CVE-2006-4566 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4566>
- Référence CVE CVE-2006-4570 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4570>

Gestion détaillée du document

15 septembre 2006 version initiale.

26 septembre 2006 ajout des références aux bulletins de sécurité SuSE, Ubuntu, Red Hat, Mandriva et SGI.

28 septembre 2006 ajout des références aux bulletins de sécurité Ubuntu, Red Hat.