Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 17 mai 2005
N° CERTA-2005-AVI-148-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des produits Mozilla

Gestion du document

Référence	CERTA-2005-AVI-148-001
Titre	Multiples vulnérabilités des produits Mozilla
Date de la première version	18 avril 2005
Date de la dernière version	17 mai 2005
Source(s)	Bulletins de sécurité Mozilla Foundation du 15 et 16 avril 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

- Exécution de code arbitraire ;
- contournement de la politique de sécurité ;
- vulnérabilité de type `cross site scripting`.

2 Systèmes affectés

- Mozilla Firefox 1.0.2 et versions antérieures ;
- Mozilla Suite 1.7.6 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités découvertes dans les produits Mozilla permettent à un utilisateur mal intentionné d'exécuter du code arbitraire, de contourner la politique de sécurité ou d'effectuer des attaques de type `cross site scripting`.

4 Description

- Une vulnérabilité découverte dans Firefox permet à un utilisateur mal intentionné d'exécuter du code arbitraire par le seul fait d'inciter l'utilisateur à installer manuellement des modules manquants (MFSA 2005-34) ;
- une vulnérabilité découverte dans les produits Mozilla permet à un individu d'exécuter du code arbitraire, en incitant l'utilisateur à afficher une fenêtre `popup` (initialement bloquée) dont l'adresse réticulaire est malicieusement constituée (MFSA 2005-35) ;
- une vulnéraibilité dans les produits Mozilla permet à un utilisateur distant mal intentionné d'effectuer des attaques de type `cross site scripting` au moyen d'un site web malicieusement construit (MFSA 2005-36) ;
- une vulnérabilité dans les produits Mozilla permet à un individu mal intentionné d'exécuter du code arbitraire sur le système vulnérable (MFSA 2005-37) ;
- une vulnérabilité découverte dans les produits Mozilla permet à un individu malveillant d'exécuter du code arbitraire au moyen d'un adresse réticulaire malicieusement constituée, initialement destinée à effectuer une recherche de modules manquants (MFSA 200-38) ;
- une vulnérabilité affectant Firefox permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'une adresse réticulaire malicieusement construite (MFSA 2005-39) ;
- une vulnérabilité découverte dans les objets `javascript` suivants : `InstallTrigger` et `XPInstall-related`. Cette vulnérabilité permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système vulnérable (MFSA 2005-40) ;
- une vulnérabilité affectant les produits Mozilla permet à un utilisateur mal intentionné d'exécuter du code arbitraire. L'exploitation de cette vulnérabilité nécessite l'interaction de la victime (MFSA 2005-41).

5 Solution

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

- Mise à jour de sécurité Firefox 1.0.3 :
  http://www.mozilla.org/products/firefox/
- Mise à jour de sécurité Mozilla 1.7.7 :
  http://www.mozilla.org/products/mozilla1.x/

6 Documentation

- Site Internet de l'éditeur :
  http://www.mozilla.org
- Bulletin de sécurité Mozilla Foundation #2005-34 du 16 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-34.html
- Bulletin de sécurité Mozilla Foundation #2005-35 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-35.html
- Bulletin de sécurité Mozilla Foundation #2005-36 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-36.html
- Bulletin de sécurité Mozilla Foundation #2005-37 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-37.html
- Bulletin de sécurité Mozilla Foundation #2005-38 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-38.html
- Bulletin de sécurité Mozilla Foundation #2005-39 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-39.html
- Bulletin de sécurité Mozilla Foundation #2005-40 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-40.html
- Bulletin de sécurité Mozilla Foundation #2005-41 du 15 avril 2005 :
  http://www.mozilla.org/security/announce/mfsa2005-41.html
- Bulletin de sécurité Mandriva MDKSA-2005:088 du 13 mai 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:088

- Bulletin de sécurité RedHat RHSA-2005-383-07 du 21 avril 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-38r34.html
- Bulletin de sécurité RedHat RHSA-2005-384-11 du 28 avril 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-384.html
- Bulletin de sécurité RedHat RHSA-2005-386-08 du 26 avril 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-386.html
- Bulletin de sécurité SuSE SUSE-SA:2005:028 du 27 avril 2005 :
  http://www.novell.com/linux/security/advisories/2005_28_mozilla_firefox.html
- Référence CVE CAN-2005-1153 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1153
- Référence CVE CAN-2005-1154 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1154
- Référence CVE CAN-2005-1155 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1155
- Référence CVE CAN-2005-1156 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1156
- Référence CVE CAN-2005-1157 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1157
- Référence CVE CAN-2005-1158 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1158
- Référence CVE CAN-2005-1159 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1159
- Référence CVE CAN-2005-1160 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1160

Gestion détaillée du document

18 avril 2005 version initiale.
17 mai 2005 ajout des références CVE et des bulletins de sécurité Mandriva, RedHat et SuSE.