Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 septembre 2004
N° CERTA-2004-AVI-320

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur les logiciels Mozilla

Gestion du document

Référence	CERTA-2004-AVI-320
Titre	Multiples vulnérabilités sur les logiciels Mozilla
Date de la première version	16 septembre 2004
Date de la dernière version	–
Source(s)	Bulletins de sécurité Mozilla
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

Les risques sont liés à chaque vulnérabilité et sont indiqués dans la description de la vulnérabilité dans la section *Description*.

2 Systèmes affectés

- Mozilla versions 0.x ;
- Mozilla version 1.0 ;
- Mozilla version 1.1 ;
- Mozilla version 1.2 ;
- Mozilla version 1.3 ;
- Mozilla version 1.4 ;
- Mozilla version 1.5 ;
- Mozilla version 1.6 ;
- Mozilla versions 1.7.x antérieures à la version 1.7.3 ;
- Mozilla Firefox versions 0.x antérieures à la version 1.0PR ;
- Mozilla Thunderbird versions 0.x antérieures à la version 0.8 ;
- Netscape versions 7.x.

3 Résumé

De multiples vulnérabilités présentes dans les logiciels Mozilla, Mozilla FireFox, Mozilla Thunderbird et Netscape permettent à un utilisateur mal intentionné d'accéder et de modifier des informations sensibles, de réaliser des attaques de type « Cross Site Scripting », de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur les systèmes où sont installés les logiciels vulnérables.

4 Description

- Plusieurs débordements de mémoire sont présents dans le fichier `nsMsgCompUtils.cpp`. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné, via un courrier éléctronique malicieusement construit, pour réaliser un déni de service ou exécuter du code arbitraire à distance.
- Un utilisateur mal intentionné peut exploiter une insuffisance dans les restrictions des actions effectuées par les scripts pour lire et écrire dans le presse-papier.
- Plusieurs débordements de mémoire sont présents dans les fichiers `writeGroup` et `nsVCardObj.cpp`. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné, via un courrier électronique contenant une carte de visite malicieusement construite, pour réaliser un déni de service ou exécuter du code arbitraire à distance.
- Plusieurs débordements de mémoire sont présents dans le fichier `nsPop3Protocol.cpp` chargé du traitement des communications POP. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné, via une réponse du serveur POP malicieusement construite, pour réaliser un déni de service ou exécuter du code arbitraire à distance. Netscape n'est pas affecté par ces vulnérabilités.
- Un utilisateur mal intentionné, par le biais d'un lien malicieusement construit dans un courrier éléctronique ou sur une page web, peut exécuter du code arbitraire ou réaliser un déni de service.
- Un utilisateur mal intentionné, par le biais d'une image au format BMP malicieusement construite dans un courrier électronique ou sur une page web, peut exécuter du code arbitraire ou réaliser un déni de service.
- Une vulnérabilité est présente dans la gestion des liens entre plusieurs fenêtres ou plusieurs cadres (`frames`). Cette vulnérabilité permet à un utilisateur mal intentionné en combinant d'autres vulnérabilités d'exécuter du code arbitraire.
- Un utilisateur mal intentionné, par l'envoi d'un paramètre malicieux, peut dissimuler le fait qu'un script signé ait été envoyé. Cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter un script signé en contournant le message d'avertissement envoyé à l'utilisateur. Netscape n'est pas affecté par cette vulnérabilité.
- Des fichiers installés par l'installeur linux sont en écriture pour tous. Cela peut être exploité par un utilisateur mal intentionné pour exécuter du code arbitraire en remplaçant certains fichiers. Netscape n'est pas affecté par cette vulnérabilité.
- Certains fichiers et répertoires dans l'archive `.tar.gz` ont des propriétaires et des privilèges inapropriés. Cette vulnérabilité peut être exploitée par un utilisateur local mal intentionné pour remplacer ces fichiers et exécuter du code arbitraire.

5 Solution

Installer les versions qui ne sont pas affectées par ces vulnérabilités :

- Mozilla version 1.7.3 ;
- Mozilla Firefox version 1.0PR ;
- Mozilla Thunderbird 0.8.

6 Documentation

- Site internet de Mozilla :
  http://www.mozilla.org
- Bulletin de sécurité Mozilla n258005 :
  http://bugzilla.mozilla.org/show_bug.cgi?id=258005
- Bulletin de sécurité Mozilla n257523 :
  http://bugzilla.mozilla.org/show_bug.cgi?id=257523

- Bulletin de sécurité Mozilla n257314 : http://bugzilla.mozilla.org/show_bug.cgi?id=257314
- Bulletin de sécurité Mozilla n245066 : http://bugzilla.mozilla.org/show_bug.cgi?id=245066
- Bulletin de sécurité Mozilla n226669 : http://bugzilla.mozilla.org/show_bug.cgi?id=226669
- Bulletin de sécurité Mozilla n256316 : http://bugzilla.mozilla.org/show_bug.cgi?id=256316
- Bulletin de sécurité Mozilla n255067 : http://bugzilla.mozilla.org/show_bug.cgi?id=255067
- Bulletin de sécurité Mozilla n250862 : http://bugzilla.mozilla.org/show_bug.cgi?id=250862
- Bulletin de sécurité Mozilla n253942 : http://bugzilla.mozilla.org/show_bug.cgi?id=253942
- Bulletin de sécurité Mozilla n231083 : http://bugzilla.mozilla.org/show_bug.cgi?id=231083
- Bulletin de sécurité Mozilla n235781 : http://bugzilla.mozilla.org/show_bug.cgi?id=235781
- Bulletin de sécurité Mozilla n254303 : http://bugzilla.mozilla.org/show_bug.cgi?id=254303

Gestion détaillée du document

16 septembre 2004 version initiale.