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 juillet 2008
N° CERTA-2008-AVI-368

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTA-2008-AVI-368
Titre	Vulnérabilités dans Mozilla Firefox
Date de la première version	17 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla MFSA 2008-36 du 16 juillet 2008 Bulletin de sécurité Mozilla MFSA 2008-35 du 15 juillet 2008 Bulletin de sécurité Mozilla MFSA 2008-34 du 15 juillet 2008
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Mozilla Firefox versions antérieures à 2.0.0.16 ;
- Mozilla Firefox 3.0.

3 Résumé

Des vulnérabilités identifiées dans `Mozilla Firefox` permettent à une personne malintentionnée de contourner la politique de sécurité, de porter atteinte à la confidentialité des données et / ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été identifiée dans les versions 2.0.0.15 et 3.0 de Mozilla Firefox. Elle permet à une personne malintentionnée de lancer des URI de type chrome: ou des URI normalement traitées par une autre application. Ceci peut être exploité pour porter atteinte à la confidentialité des données.

Une deuxième faille dans Mozilla Firefox 3.0 permet d'injecter des *scripts* dans des documents chrome. Cette attaque permet à un attaquant de contourner la politique de sécurité. Couplée avec la première vulnérabilité, cette faille permettrait également d'exécuter du code arbitraire.

Une troisième vulnérabilité a été identifiée dans les deux branches de Mozilla Firefox. Elle concerne un compteur de taille insuffisante utilisé pour référencer des objets CSS. Ceci peut être exploité par une personne malintentionnée pour exécuter du code arbitraire à distance.

Enfin, une quatrième vulnérabilité concerne le traitement des GIF dans Mozilla Firefox 3.0 sous Mac OS X. Une personne malintentionnée pourrait ainsi exécuter du code arbitraire à distance via un fichier GIF spécialement conçu.

5 Solution

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

6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-36 du 16 juillet 2008 :
  http://www.mozilla.org/security/announce/2008/MFSA2008-36.html
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-35 du 15 juillet 2008 :
  http://www.mozilla.org/security/announce/2008/MFSA2008-35.html
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-34 du 15 juillet 2008 :
  http://www.mozilla.org/security/announce/2008/MFSA2008-34.html
- Note de vulnérabilité de l'US-CERT VU#130923 du 16 juillet 2008 :
  http://www.kb.cert.org/vuls/id/130923
- Référence CVE CVE-2008-2934 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2934
- Référence CVE CVE-2008-2933 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2933
- Référence CVE CVE-2008-2785 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2785
- Référence CVE CVE-2008-2786 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2786

Gestion détaillée du document

17 juillet 2008 version initiale.