Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juin 2009
N° CERTA-2009-AVI-251

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du client de messagerie Mozilla Thunderbird

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-2009-AVI-251

Gestion du document

Référence	CERTA-2009-AVI-251
Titre	Multiples vulnérabilités du client de messagerie Mozilla Thunderbird
Date de la première version	24 juin 2009
Date de la dernière version	–
Source(s)	Bulletins de mise à jour Mozilla Thunderbird du 23 juin 2009
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Mozilla Thunderbird versions antérieures à la version 2.0.22.

3 Résumé

De multiples vulnérabilités permettant entre autre d'exécuter du code arbitraire à distance ont été découvertes dans `Mozilla Thunderbird`.

4 Description

De multiples vulnérabilités ont été découvertes dans le client de messagerie `Mozilla Thunderbird`. L'exploitation de ces vulnérabilités permet de réaliser un grand nombre d'actions malveillantes, dont l'exécution de code arbitraire à distance ou le déni de service à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-24 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-24.html
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-27 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-27.html
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-29 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-29.html
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-31 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-31.html
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-32 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-32.html
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-33 du 23 juin 2009 :
  http://www.mozilla.org/security/announce/2009/mfsa2009-33.html
- Référence CVE CVE-2009-1392 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1392
- Référence CVE CVE-2009-1832 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1832
- Référence CVE CVE-2009-1833 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1833
- Référence CVE CVE-2009-1836 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1836
- Référence CVE CVE-2009-1838 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1838
- Référence CVE CVE-2009-1840 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1840
- Référence CVE CVE-2009-1841 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1841

Gestion détaillée du document

24 juin 2009 version initiale.