



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mars 2009
N° CERTA-2009-AVI-109

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-109>

Gestion du document

Référence	CERTA-2009-AVI-109
Titre	Multiples vulnérabilités dans Mozilla Thunderbird
Date de la première version	23 mars 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité MFSA2009-01, MFSA2009-07, MFSA2009-09, MFSA2009-10
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 Thunderbird versions antérieures à la 2.0.0.21.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans Mozilla Thunderbird et permettent notamment d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Mozilla Thunderbird :

- le moteur des produits Mozilla comporte plusieurs défauts et permet à un utilisateur malveillant de réaliser une exécution de code arbitraire à distance ;
- un traitement défectueux permet à un site malveillant de lire sans autorisation des informations au format XML provenant d'un autre domaine ;
- des erreurs dans la bibliothèque de traitement des images au format PNG permettent à un utilisateur malveillant d'exécuter du code arbitraire 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/MFSA2009-01 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-01.html>
- Bulletin de sécurité de la fondation Mozilla 2009/MFSA2009-07 du 04 mars 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>
- Bulletin de sécurité de la fondation Mozilla 2009/MFSA2009-09 du 04 mars 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-09.html>
- Bulletin de sécurité de la fondation Mozilla 2009/MFSA2009-10 du 04 mars 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-10.html>
- Référence CVE CVE-2009-0040 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040>
- Référence CVE CVE-2009-0352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0352>
- Référence CVE CVE-2009-0353 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0353>
- Référence CVE CVE-2009-0771 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0771>
- Référence CVE CVE-2009-0772 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0772>
- Référence CVE CVE-2009-0773 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0773>
- Référence CVE CVE-2009-0774 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0774>
- Référence CVE CVE-2009-0776 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0776>

Gestion détaillée du document

23 mars 2009 version initiale.