Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 janvier 2010
N° CERTA-2010-AVI-024

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mozilla Thunderbird 3.0

Gestion du document

Référence	CERTA-2010-AVI-024
Titre	Multiples vulnérabilités dans Mozilla Thunderbird 3.0
Date de la première version	21 janvier 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité Mozilla MFSA2009-65, MFSA2009-66, MFSA2009-67
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.

2 Systèmes affectés

Mozilla Thunderbird 3.0

3 Résumé

De multiples vulnérabilités dans `Mozilla Thunderbird` permettent l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans `Mozilla Thunderbird`:

– plusieurs problèmes de stabilité affectent le moteur de rendu. Certains mènent à une corruption de la mémoire et permettent l'exécution de code arbitraire à distance ;

– des failles dans la bibliothèque `liboggplay` permettent l'exécution de code arbitraire à distance ;
– une vulnérabilité de type débordement d'entier dans la bibliothèque `libtheora` permet l'exécution de code arbitraire à distance. Un autre problème dans cette bibliothèque peut être exploité pour provoquer un déni de service à distance.

Il est à noté que ces vulnérabilités avaient déjà été corrigées dans `Mozilla Thunderbird 3.5.6` et `Mozilla SeaMonkey 2.0.1` (voir l'avis CERTA-2009-AVI-547).

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/MFSA2009-65 :
http://www.mozilla.org/security/announce/2009/mfsa2009-65.html
– Bulletin de sécurité de la fondation Mozilla 2009/MFSA2009-66 :
http://www.mozilla.org/security/announce/2009/mfsa2009-66.html
– Bulletin de sécurité de la fondation Mozilla 2009/MFSA2009-67 :
http://www.mozilla.org/security/announce/2009/mfsa2009-67.html
– Référence CVE CVE-2009-3388 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3388
– Référence CVE CVE-2009-3389 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3389
– Référence CVE CVE-2009-3379 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3379
– Référence CVE CVE-2009-3380 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3380
– Référence CVE CVE-2009-3381 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3381
– Référence CVE CVE-2009-3382 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3382

Gestion détaillée du document

21 janvier 2010 version initiale.