

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-2008-AVI-376>

Gestion du document

Référence	CERTA-2008-AVI-376
Titre	Multiples vulnérabilités du client de messagerie Mozilla Thunderbird
Date de la première version	25 juillet 2008
Date de la dernière version	–
Source(s)	Note de version Thunderbird du 23 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Mozilla Thunderbird version 2.0.15 et versions antérieures.

3 Résumé

De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. L'exploitation de ces vulnérabilités permet des actions diverses, dont le déni de service à distance, le contournement de la politique de sécurité, ou l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans le client mail Mozilla Thunderbird. Ces vulnérabilités peuvent être exploitées à distance afin de conduire de nombreuses actions malveillantes, dont l'exécution de code arbitraire.

5 Solution

Se référer à la note de version de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Note de version Mozilla Thunderbird du 23 juillet 2008 :
<http://www.mozilla-europe.org/fr/products/thunderbird/2.0.0.16/releasenotes>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-26 du 23 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-26.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-34 du 15 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-34.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-33 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-33.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-31 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-31.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-29 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-29.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-25 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-25.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-24 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-24.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFS2008-21 du 01 juillet 2008 :
<http://www.mozilla.org/security/announce/2008/MFS2008-21.html>
- Référence CVE CVE-2008-2785 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2785>
- Référence CVE CVE-2008-2811 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2811>
- Référence CVE CVE-2008-2809 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2809>
- Référence CVE CVE-2008-2807 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2807>
- Référence CVE CVE-2008-2803 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2803>
- Référence CVE CVE-2008-2802 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2802>
- Référence CVE CVE-2008-2799 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2799>
- Référence CVE CVE-2008-2798 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2798>

Gestion détaillée du document

25 juillet 2008 version initiale.