

Affaire suivie par :
CERTA

BULLETIN D'ALERTE 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-ALE-014>

Gestion du document

Référence	CERTA-2009-ALE-014-001
Titre	Multiples vulnérabilités du client de messagerie Mozilla Thunderbird
Date de la première version	07 août 2009
Date de la dernière version	25 août 2009
Source(s)	Bulletins de sécurité Mozilla MFSA2009-18, MFSA2009-19, MFSA2009-31, MFSA2009-34, MFSA2009-42, MFSA2009-43
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 ;
- élévation de privilèges ;
- injection de code indirecte.

2 Systèmes affectés

- Mozilla Thunderbird version 2.0.0.23 et versions antérieures.

3 Résumé

De multiples vulnérabilités conduisant, entre autres, à une exécution de code arbitraire à distance ont été découvertes dans Mozilla Thunderbird.

4 Description

De multiples vulnérabilités sont présentes dans la version 2.0.0.23 et dans les versions antérieures du client de messagerie Mozilla Thunderbird. Ces vulnérabilités permettent de réaliser des actions malveillantes telles que le contournement de la politique de sécurité, l'élévation de privilège, ou encore l'exécution de code arbitraire à distance.

Pour le détail de chaque vulnérabilité, se reporter aux bulletins de sécurité de l'éditeur (cf. section Documentation).

5 Contournement provisoire

Dans l'attente de la sortie des correctifs, le CERTA recommande :

- de laisser inactive l'interprétation des javascript (option par défaut) ;
- d'utiliser un moyen de chiffrement autre que construit autour de l'utilisation de certificats SSL directement par Mozilla Thunderbird.

Note : la vulnérabilité décrite dans le bulletin MFSA2009-42 a été corrigée dans la version 2.0.0.23 du client de messagerie.

6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-18 du 21 avril 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-18.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-19 du 21 avril 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-19.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-31 du 11 juin 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-31.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-34 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-42 du 01 août 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-42.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-43 du 01 août 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-43.html>
- Bulletin d'actualité du CERTA numéro CERTA-2009-ACT-032 du 07 août 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-032/index.html>
- Référence CVE CVE-2009-1308 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1308>
- Référence CVE CVE-2009-1309 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1309>
- Référence CVE CVE-2009-1840 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1840>
- Référence CVE CVE-2009-2462 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2462>
- Référence CVE CVE-2009-2463 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2463>
- Référence CVE CVE-2009-2464 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2464>
- Référence CVE CVE-2009-2465 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2465>
- Référence CVE CVE-2009-2466 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2466>
- Référence CVE CVE-2009-2408 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408>
- Référence CVE CVE-2009-2404 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2404>

Gestion détaillée du document

07 août 2009 version initiale ;

25 août 2009 prise en compte de la version 2.0.0.23.