

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Metamail

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-2006-AVI-109>

Gestion du document

Référence	CERTA-2006-AVI-109-001
Titre	Vulnérabilité dans Metamail
Date de la première version	14 mars 2006
Date de la dernière version	20 mars 2006
Source(s)	Rapport d'erreur Debian du 12 février 2006
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.

2 Systèmes affectés

Metamail 2.7.x.

3 Résumé

Une vulnérabilité dans Metamail permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Une vulnérabilité de type débordement de tampon dans Metamail permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire sur la machine vulnérable par le biais d'un courrier électronique malicieusement construit.

5 Solution

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

6 Documentation

- Rapport d'erreur Debian du 12 février 2006 :
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=352482>
- Bulletin de sécurité Debian DSA 995 du 13 mars 2006 :
<http://www.debian.org/security/dsa-995>
- Bulletin de sécurité Mandriva MDKSA-2006:047 du 22 février 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:047>
- Bulletin de sécurité RedHat RHSA-2006:0217 du 21 février 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0217.html>
- Bulletin de sécurité SUSE SuSE-SA:2006:005 du 03 mars 2006 :
http://www.novell.com/linux/security/advisories/2006_05_sr.html
- Bulletin de sécurité Gentoo GLSA 200603-16 du 17 mars 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200603-16.xml>
- Référence CVE CVE-2006-0709 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0709>

Gestion détaillée du document

14 mars 2006 version initiale.

20 mars 2006 ajout de la référence au bulletin de sécurité Gentoo.