



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 juin 2005  
N° CERTA-2005-AVI-186-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Mailutils

---

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-2005-AVI-186>

---

### Gestion du document

Référence	CERTA-2005-AVI-186-001
Titre	Multiples vulnérabilités dans Mailutils
Date de la première version	30 mai 2005
Date de la dernière version	06 juin 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200505-20 du 27 mai 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Exécution de code arbitraire ;
- déni de service.

## 2 Systèmes affectés

mailutils 0.6r1 et versions antérieures.

## 3 Résumé

De nombreuses vulnérabilités découvertes dans mailutils permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou d'effectuer un déni de service.

## 4 Description

Mailutils est une suite de bibliothèques et d'utilitaires destinés à traiter les messages électroniques.

- Une vulnérabilité de type débordement de mémoire dans le binaire Mail permet à un individu distant malveillant d'exécuter du code arbitraire avec les privilèges de la victime (CAN-2005-1520) ;

- une vulnérabilité de type débordement de mémoire présente dans la fonction `fetch_io()` permet à une personne mal intentionnée d'exécuter du code arbitraire à distance (CAN-2005-1521) ;
- une vulnérabilité dans le traitement des paramètres de la commande `FETCH` permet à un utilisateur malveillant d'effectuer un déni de service à distance en consommant toutes les ressources CPU du système (CAN-2005-1522) ;
- une vulnérabilité de type chaîne de format dans le serveur `imap4d` permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire (CAN-2005-1523).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité iDEFENSE #246 du 25 mai 2005 :  
<http://www.idefense.com/application/poi/display?id=246&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #247 du 25 mai 2005 :  
<http://www.idefense.com/application/poi/display?id=247&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #248 du 25 mai 2005 :  
<http://www.idefense.com/application/poi/display?id=248&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE #249 du 25 mai 2005 :  
<http://www.idefense.com/application/poi/display?id=249&type=vulnerabilities>
- Bulletin de sécurité Gentoo GLSA 200505-20 du 27 mai 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200505-20.xml>
- Bulletin de sécurité Debian DSA-732 du 03 juin 2005 :  
<http://www.debian.org/security/2005/dsa-732>
- Référence CVE CAN-2005-1520 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1520>
- Référence CVE CAN-2005-1521 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1521>
- Référence CVE CAN-2005-1522 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1522>
- Référence CVE CAN-2005-1523 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1523>

## Gestion détaillée du document

**30 mai 2005** version initiale.

**06 juin 2005** ajout référence au bulletin de sécurité Debian.