

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Mailman

---

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-066>

---

### Gestion du document

Référence	CERTA-2005-AVI-066-004
Titre	Vulnérabilité de Mailman
Date de la première version	11 février 2005
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200502-11 du 10 février 2005
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

- Accès à des informations non autorisées ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

Mailman version 2.1.5 et versions antérieures.

## 3 Description

Mailman est un logiciel permettant la gestion des listes de diffusion.  
Une vulnérabilité dans la fonction `true_path` du fichier `private.py` permet à un utilisateur mal intentionné de réaliser une traversée de répertoires pouvant conduire à l'accès à des fichiers non autorisés.

## 4 Solution

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

## 5 Documentation

- Site Internet de Mailman :  
<http://www.gnu.org/software/mailman/mailman.html>
- Bulletin de sécurité Gentoo GLSA 200502-11 du 10 février 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200502-11.xml>
- Bulletin de sécurité Debian DSA-674 du 10 février 2005 :  
<http://www.debian.org/security/2005/dsa-674>
- Bulletin de sécurité RedHat RHSA-2005:136 du 10 février 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-136.html>
- Bulletin de sécurité RedHat RHSA-2005:137 du 15 février 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-137.html>
- Bulletin de sécurité OpenBSD pour mailman du 10 février 2005 :  
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité FreeBSD pour mailman du 12 février 2005 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Mandrake MDKSA-2005:037 du 14 février 2005 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:037>
- Bulletin de sécurité SUSE SUSE-SA:2005:007 du 14 février 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_07\\_mailman.html](http://www.novell.com/linux/security/advisories/2005_07_mailman.html)
- Mise à jour de sécurité du paquetage NetBSD mailman :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/mailman/README.html>
- Référence CVE CAN-2005-0202 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0202>

### Gestion détaillée du document

**11 février 2005** version initiale.

**14 février 2005** ajout de la référence au bulletin de sécurité FreeBSD.

**15 février 2005** ajout des références aux bulletins de sécurité Mandrake MDKSA-2005:037 et SUSE SUSE-SA:2005:007.

**15 février 2005** ajout de la référence au bulletin de sécurité NetBSD.

**17 février 2005** ajout de la référence au bulletin de sécurité RedHat RHSA-2005:137.