

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-041>

---

### Gestion du document

Référence	CERTA-2005-AVI-041-002
Titre	Vulnérabilité de mailman
Date de la première version	31 janvier 2005
Date de la dernière version	01 mars 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200501-29
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 scripts arbitraires à distance.

## 2 Systèmes affectés

Toutes les versions de Mailman, y compris la dernière version 2.1.5 (sortie le 15 mai 2004).

## 3 Description

Mailman est un logiciel permettant la gestion des listes de diffusion.  
Une vulnérabilité dans Mailman permet à un utilisateur mal intentionné d'exécuter des scripts arbitraires à distance dans le contexte du navigateur de la victime (cross-site scripting).

## 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 200501-29 du 22 janvier 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200501-29.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:015 du 24 janvier 2005 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:015>
- Bulletin de sécurité OpenBSD pour mailman du 26 janvier 2005 :  
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité Debian DSA-674 du 10 février 2005 :  
<http://www.debian.org/security/2005/dsa-674>
- Mise à jour de sécurité du paquetage NetBSD mailman :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/mailman/README.html>
- Référence CVE CAN-2004-1143 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1143>
- Référence CVE CAN-2004-1177 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1177>

### Gestion détaillée du document

**31 janvier 2005** version initiale.

**10 février 2005** ajout de la référence au bulletin de sécurité Debian DSA-674.

**01 mars 2005** ajout de la référence au bulletin de sécurité NetBSD.