



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 mai 2004  
N° CERTA-2004-AVI-026-005

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans 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-2004-AVI-026>

---

## Gestion du document

Référence	CERTA-2004-AVI-026-005
Titre	Vulnérabilité dans mailman
Date de la première version	09 février 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité RedHat RHSA-2004:020-02
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

- Usurpation d'identité ;
- perte de confidentialité des données.

## 2 Systèmes affectés

Toutes les versions de mailman antérieures à la version 2.1.4.

## 3 Résumé

Deux vulnérabilités de type `cross-site scripting` sont présentes dans mailman.

## 4 Description

mailman est un logiciel permettant la gestion des listes de diffusion. Un utilisateur mal intentionné peut exploiter deux vulnérabilités afin d'exécuter des scripts sur un poste client accédant à l'application mailman vulnérable au travers de son navigateur (vulnérabilité de type `cross-site scripting`). Il est alors possible de récupérer les données d'authentification du poste client ou de lire les données transmises au site vulnérable par l'utilisateur.

## 5 Solution

Mettre à jour mailman en version 2.1.4. Se référer à la section Documentation pour la mise à jour selon la distribution concernée.

## 6 Documentation

- Site internet de mailman :  
<http://www.list.org>
- Avis de sécurité RedHat RHSA-2004:019 :  
<http://rhn.redhat.com/errata/RHSA-2004-019.html>
- Avis de sécurité RedHat RHSA-2004:020 :  
<http://rhn.redhat.com/errata/RHSA-2004-020.html>
- Avis de sécurité RedHat RHSA-2004:156 :  
<http://rhn.redhat.com/errata/RHSA-2004-156.html>
- Avis de sécurité Debian DSA-436 :  
<http://www.debian.org/security/2004/dsa-436> Le correctif proposé par Debian dans l'avis DSA-436 introduit une nouvelle vulnérabilité.
- Avis de sécurité Mandrake MDKSA-2004:013 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:013>
- Avis de sécurité SUSE SuSE:2004:008 su 14 avril 2004 :  
[http://www.suse.com/de/security/2004\\_08\\_cvs.html](http://www.suse.com/de/security/2004_08_cvs.html)
- Avis de sécurité SGI 20040201-01-U du 11 février 2004 :  
<ftp://patches.sgi.com/support/free/security/advisories/20040201-01-U.asc>
- Avis de sécurité SGI 20040404-01-U du 21 avril 2004 :  
<ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc>
- Quatre avis de sécurité FreeBSD du 25 février 2004 :  
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD mailman :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2003-0038 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0038>
- Référence CVE CAN-2003-0965 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0965>
- Référence CVE CAN-2003-0991 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0991>
- Référence CVE CAN-2003-0992 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0992>
- Référence CVE CAN-2004-0182 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0182>

## Gestion détaillée du document

**09 février 2004** version initiale.

**16 février 2004** ajout du bulletin de sécurité de Mandrake.

**24 février 2004** modification de l'avis Debian. Le précédent correctif Debian (DSA-436-1) introduit une nouvelle vulnérabilité.

**08 mars 2004** ajout du bulletin de sécurité de Fedora.

**10 mai 2004** ajout des références aux bulletins de sécurité RedHat, SUSE, SGI et ajout d'une nouvelle référence CVE.

**12 mai 2004** ajout des références aux bulletins de sécurité FreeBSD et NetBSD.