

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités 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-2006-AVI-426>

Gestion du document

Référence	CERTA-2006-AVI-426
Titre	Multiples Vulnérabilités dans Mailman
Date de la première version	05 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian du 04 octobre 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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Mailman version 2.1.9rc1 et antérieures.

3 Résumé

De multiples vulnérabilités dans Mailman permettent à un utilisateur distant d'injecter du code dans une ou plusieurs pages du site vulnérable ainsi que de modifier les journaux d'événements.

4 Description

Deux vulnérabilités sont présentes dans Mailman :

- La première vulnérabilité est de type *Injection de code indirecte (Cross Site Scripting)*. Elle peut être exploitée par une personne mal intentionnée afin d'injecter du code dans une ou plusieurs pages du site vulnérable.

- La seconde vulnérabilité concerne la fonction `Utils.py`. Elle permet à un utilisateur distant d’injecter des messages arbitraires dans les journaux d’événements.

5 Solution

La version 2.1.9 de Mailman corrige les vulnérabilités. Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 1188 du 04 octobre 2006 :
<http://www.debian.org/security/2006/dsa-1188>
- Annonce Mailman du 12 septembre 2006 :
<http://mail.python.org/pipermail/mailman-announce/2006-september/000087.html>
- Bulletin de sécurité Mandriva MDKSA-2006:165 du 18 septembre 2006 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:165>
- Bulletin de sécurité RedHat RHSA-2006:0600 du 06 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0600.html>
- Référence CVE CVE-2006-3636 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3636>
- Référence CVE CVE-2006-4624 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4624>

Gestion détaillée du document

05 octobre 2006 version initiale.