Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2002
N° CERTA-2002-AVI-197

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-2002-AVI-197

Gestion du document

Référence	CERTA-2002-AVI-197
Titre	Vulnérabilité de mailman
Date de la première version	30 août 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité DSA-147 de Debian.
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

Mailman versions 2.0.11 et antérieures.

3 Résumé

Une vulnérabilité de type `cross-site scripting` est présente dans un des scripts CGI de mailman.

4 Description

Mailman est un logiciel permettant de gérer des listes de diffusion.

Le script CGI `ml-name` ne filtre pas correctement les données reçues.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité 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

La version 2.0.12 de mailman corrige cette vulnérabilité.

6 Documentation

- Site de mailman :
  http://www.gnu.org/software/mailman
- Message "Released Mailman 2.0.12" sur la liste de diffusion Mailman-Developper :
  http://python.org/msg03563.html
- Bulletin de sécurité DSA-147 de Debian :
  http://www.debian.org/security/2002/dsa-147
- Bulletin de sécurité RHSA-2002:176 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2002-176.html
- Note d'information CERTA-2002-INF-001 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html

Gestion détaillée du document

30 août 2002 version initiale.