

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans spamass-milter

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-2010-AVI-135>

Gestion du document

Référence	CERTA-2010-AVI-135
Titre	Vulnérabilité dans spamass-milter
Date de la première version	26 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-2021-1 du 22 mars 2010
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 code arbitraire à distance.

2 Systèmes affectés

Spamass-milter 0.3.1 et versions antérieures.

3 Résumé

Une vulnérabilité dans spamass-milter permet l'exécution de code arbitraire à distance.

4 Description

Spamass-milter est un module de spamassassin permettant de l'utiliser avec des serveurs de messagerie comme Sendmail ou Postfix. Une vulnérabilité de ce produit permet à une personne malintentionnée d'exécuter du code arbitraire. Ceci n'est possible que si l'option `-x` est activée (ce qui n'est pas le cas par défaut).

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 2021 du 22 mars 2010 :
<http://www.debian.org/security/2010/dsa-2021>

Gestion détaillée du document

26 mars 2010 version initiale.