



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juin 2006
N° CERTA-2006-AVI-234-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans SpamAssassin

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-234>

Gestion du document

Référence	CERTA-2006-AVI-234-001
Titre	Vulnérabilités dans SpamAssassin
Date de la première version	12 juin 2006
Date de la dernière version	27 juin 2006
Source(s)	
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.

2 Systèmes affectés

SpamAssassin versions:

- 2.5.x;
- 2.6.x;
- 3.0.x;
- 3.1.x.

3 Résumé

Une vulnérabilité a été publiée dans le logiciel anti-spam SpamAssassin. Elle permet l'exécution de code arbitraire à distance.

4 Description

Pour que la vulnérabilité soit mise en oeuvre il est nécessaire que les directives `-vpopmail` et `-paranoid` soit activées dans le fichier de configuration. Il est à noter qu'il ne s'agit pas de la configuration par défaut.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Nouvelle version de SpamAssassin
<http://spamassassin.apache.org/downloads.cgi?update=200606050750>
- Bulletin de sécurité Debian DSA-1090 du 06 juin 2006 :
<http://www.debian.org/security/2006/dsa-1090>
- Bulletin de sécurité RedHat RHSA-2006:0543 du 06 juin 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0543.html>
- Bulletin de sécurité Gentoo GLSA-200606-09 du 11 juin 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200606-09.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:103 du 14 juin 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:103>
- Référence CVE CAN-2006-2447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-2447>

Gestion détaillée du document

12 juin 2006 version initiale.

27 juin 2006 ajout des références aux bulletins de sécurité Debian, RedHat, Gentoo et Mandriva.