Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 mars 2006
N° CERTA-2005-AVI-457-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faiblesse de SpamAssassin

Gestion du document

Référence	CERTA-2005-AVI-457-002
Titre	Déni de service sur SpamAssassin
Date de la première version	16 novembre 2005
Date de la dernière version	08 mars 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

- Contournement de la politique de sécurité ;
- dégradation du filtrage du pourriel.

2 Systèmes affectés

Tout système utilisant *SpamAssassin*, en version source antérieure à la 3.1.0, pour filtrer les pourriels.

3 Résumé

Un utilisateur mal intentionné peut transmettre des messages volontairement mal formés qui vont provoquer un déni de service du processus d'analyse ce qui va empêcher l'identification comme pourriel.

4 Description

SpamAssassin est un service de filtrage du courrier indésirable, écrit en *Perl*.

Une expression régulière peu précise du code d'analyse des entêtes peut générer une explosion combinatoire et arrêter le processus en cours. Seul le fils analysant le message courant est impacté, pas l'ensemble du service.

5 Solution

Mettre à jour en version source 3.1.0 au moins, ou se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Gentoo Linux : la version 3.1.0 est stable pour la plupart des architectures depuis le 14 novembre 2005.

6 Documentation

- Site internet de *SpamAssassin* :
  http://spamassassin.apache.org
- Linux Fedora :
  - Fedora Core 3 du 09 novembre 2005 :
    http://www.redhat.com/archives/fedora-announce-list/2005-November/msg00028.html
  - Fedora Core 4 du 09 novembre 2005 :
    http://www.redhat.com/archives/fedora-announce-list/2005-November/msg00029.html
- Bulletin de sécurité Mandriva MDKSA-2005:221 du 02 décembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:221
- Bulletin de sécurité RedHat RHSA-2006:0129 du 07 mars 2006 :
  https://rhn.redhat.com/errata/RHSA-2006-0129.html
- Référence CVE CVE-2005-3351 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3351

Gestion détaillée du document

16 novembre 2005 version initiale.
05 décembre 2005 ajout de la référence au bulletin de sécurité Mandriva.
08 mars 2006 ajout de la référence au bulletin de sécurité RedHat.