



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2005
N° CERTA-2005-AVI-078-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'application *sympa*

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-2005-AVI-078>

Gestion du document

Référence	CERTA-2005-AVI-078-002
Titre	Vulnérabilité de l'application <i>sympa</i>
Date de la première version	15 février 2005
Date de la dernière version	10 juin 2005
Source(s)	Bulletin de sécurité Debian DSA-677 du 11 février 2005
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

- Application *sympa* version 4.1.2 et versions antérieures ;
- application *sympa* versions 5.0b et 5.0b1.

3 Résumé

Une vulnérabilité de l'application *sympa* permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable avec les privilèges de l'application *sympa*.

4 Description

L'application *sympa* est un outil de gestion de listes de diffusion.
Une vulnérabilité de type débordement de mémoire dans les programmes *queue* et *bouncequeue* permet à un utilisateur local mal intentionné d'exécuter du code arbitraire sur le système vulnérable. Le code sera exécuté avec les privilèges de l'application *sympa*.

5 Solution

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

6 Documentation

- Site Internet de `sympa` :
<http://www.sympa.org>
- Bulletin de sécurité Debian DSA-677 du 11 février 2005 :
<http://www.debian.org/security/2005/dsa-677>
- Mise à jour de sécurité du paquetage NetBSD `sympa` :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/sympa/README.html>
- Bulletin de sécurité FreeBSD pour `sympa` du 01 juin 2005 :
<http://www.vuxml.org/freebsd/pkg-sympa.html>
- Référence CVE CAN-2005-0073
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0073>

Gestion détaillée du document

15 février 2005 version initiale.

18 février 2005 ajout de la référence au site Internet de `sympa`. Ajout de la référence au bulletin de sécurité NetBSD. Corrections d'imprécisions sur la nature de la vulnérabilité ainsi que les versions de `sympa` impactées.

10 juin 2005 ajout de la référence au bulletin de sécurité FreeBSD.