

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du paquetage ipsec-tools

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-504>

Gestion du document

Référence	CERTA-2005-AVI-504-002
Titre	Vulnérabilité du paquetage ipsec-tools
Date de la première version	22 décembre 2005
Date de la dernière version	08 février 2006
Source(s)	Avis de sécurité 273756/NISCC/ISAKMP de l'UNIRAS
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

Déni de service à distance.

2 Systèmes affectés

Tout système Unix utilisant le service `racoon`, inclus dans les `ipsec-tools` dans une version source antérieure à 0.6.3.

3 Résumé

Un utilisateur mal intentionné peut envoyer des paquets volontairement mal formés au service `racoon` pour provoquer son arrêt et empêcher ainsi l'établissement de toute nouvelle connexion.

4 Description

`ipsec-tools` est une solution IPsec pour système d'exploitation Unix.

Une faille dans le gestionnaire `racoon` des associations de sécurité peut être exploitée pour provoquer un déni de service lorsque la négociation en mode agressif est configurée.

5 Solution

Mettre à jour les sources en version 0.6.3 au moins ou se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site internet des `ipsec-tools` :
<http://ipsec-tools.sourceforge.net>
- Alerte de l'UNIRAS Id:20051114-01013 du 14 novembre 2005 :
<http://www.uniras.gov.uk/niscc/docs/br-20051114-01013.html>
- Bulletin de sécurité Ubuntu USN-221-1 du 01 décembre 2005 :
<http://www.ubuntulinux.org/usn/usn-221-1>
- Bulletin de sécurité Gentoo GLSA-200512-04 du 12 décembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200512-04.xml>
- Bulletin de sécurité SUSE SuSE-SA:2005:070 du 20 décembre 2005 :
http://www.novell.com/linux/security/advisories/2005_70_ipsec.html
- Bulletin de sécurité Mandriva MDKSA-2006:020 du 25 janvier 2006 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:020>
- Bulletin de sécurité Debian DSA-965 du 6 février 2006
<http://www.debian.org/security/security/2006/dsa-965>
- Référence CVE CAN-2005-3732 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3732>

Gestion détaillée du document

22 décembre 2005 version initiale.

26 janvier 2006 ajout de la référence au bulletin de sécurité Mandriva.

08 février 2006 ajout de la référence au bulletin de sécurité Debian.