

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2008-AVI-467>

Gestion du document

Référence	CERTA-2008-AVI-467
Titre	Vulnérabilité dans IPsec-Tools
Date de la première version	18 septembre 2008
Date de la dernière version	–
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

Déni de service à distance.

2 Systèmes affectés

IPsec-Tools 0.7.1 et versions antérieures.

3 Résumé

Deux vulnérabilités permettant d'effectuer un déni de service à distance ont été corrigées dans IPsec-Tools.

4 Description

Deux vulnérabilités ont été corrigées dans IPsec-tools. La première faille est due à une fuite mémoire dans le démon `raccoon` et concerne les versions antérieures à 0.7.1 (CVE-2008-3651). La deuxième vulnérabilité concerne en plus la version 0.7.1 et est causée par une mauvaise gestion des ressources lors de la réception de paquets invalides (CVE-2008-3652). Ces deux failles peuvent être exploitées par une personne malintentionnée pour effectuer un déni de service à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Red Hat RHSA-2008-0849 du 27 août 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0849.html>
- Bulletin de sécurité Ubuntu USN-641-1 du 09 septembre 2008 :
<https://lists.ubuntu.com/archives/ubuntu-security-announce/2008-September/000746.html>
- Référence CVE CVE-2008-3651 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3651>
- Référence CVE CVE-2008-3652 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3652>

Gestion détaillée du document

18 septembre 2008 version initiale.