



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 septembre 2004
N° CERTA-2004-AVI-259-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de KAME Racoon

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-2004-AVI-259>

Gestion du document

Référence	CERTA-2004-AVI-259-001
Titre	Vulnérabilité de KAME Racoon
Date de la première version	30 juillet 2004
Date de la dernière version	08 septembre 2004
Source(s)	Bulletin de sécurité RHSA-2004:308 de Red Hat Bulletin de sécurité GLSA 200406-17 de Gentoo
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.

2 Systèmes affectés

Versions d'IPsec-tools antérieures à 0.3.3.

3 Description

KAME Racoon est le service chargé de négocier les associations de sécurité (SA) pour IPSec (utilisation des protocoles ISAKMP et IKE).

KAME Racoon ne vérifie pas correctement les signatures associées aux certificats au format X.509. Il est alors possible pour un utilisateur distant mal intentionné de s'authentifier et réaliser une connexion en violation de la politique de sécurité.

4 Solution

La version 0.3.3 d'IPsec-tools corrige cette vulnérabilité.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

5 Documentation

- Site Internet d'IPsec tools :
<http://sourceforge.net/projects/ipsec-tools>
- Bulletin de sécurité Red Hat RHSA-2004:308 du 29 juillet 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-308.html>
- Bulletin de sécurité Gentoo GLSA 200406-17 du 22 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-17.xml>
- Bulletin de sécurité Apple du 07 septembre 2004 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-0607 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0607>

Gestion détaillée du document

30 juillet 2004 version initiale.

30 juillet 2004 ajout de la référence CVE CAN-2004-0607.

08 septembre 2004 ajout de la référence au bulletin de sécurité Apple.