Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2004
N° CERTA-2004-AVI-136-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de KAME Racoon

Gestion du document

Référence	CERTA-2004-AVI-136-003
Titre	Vulnérabilité de KAME Racoon
Date de la première version	20 avril 2004
Date de la dernière version	15 juillet 2004
Source(s)	Bulletin de sécurité FreeBSD Vuxml du 14 avril 2004
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.

2 Systèmes affectés

KAME Racoon versions antérieures à la version 20040408a.

3 Résumé

Une vulnérabilité du service *KAME Racoon* permet à un utilisateur mal intentionné de provoquer un déni de service.

4 Description

KAME est une mise en oeuvre des protocoles IPSec et IPv6 sur les plates-formes BSD.
KAME Racoon est le service chargé de négocier les associations de sécurité (SA) pour IPSec (utilisation des protocoles ISAKMP et IKE).
Un mauvais traitement du champ *longueur* des en-têtes des paquets ISAKMP permet à un utilisateur distant mal intentionné d'utiliser une grande partie de la mémoire du système. Cela peut provoquer l'arrêt brutal du service.

5 Solution

La version 20040408a corrige cette vulnérabilité.
Appliquer le correctif proposé sur le site de KAME (cf. section Documentation).

6 Documentation

- Correctif proposé sur le site de KAME :
  http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/racoon/isakmp.c.diff?r1=1.180&r2=1.181
- Bulletin de sécurité FreeBSD du 14 avril 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Gentoo GLSA 200404-17 du 24 avril 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200404-17.xml
- Bulletin de sécurité RedHat RHSA-2004:165 du 11 mai 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-165.html
- Bulletin de sécurité Mandrake MDKSA-2004:069 du 14 juillet 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:069
- Référence CVE CAN-2004-0403 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0403

Gestion détaillée du document

20 avril 2004 version initiale.
26 avril 2004 correction de la référence CVE. Ajout de la référence au bulletin de sécurité Gentoo.
13 mai 2004 ajout de la référence au bulletin de sécurité RedHat.
15 juillet 2004 ajout de la référence au bulletin de sécurité Mandrake.