

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service IKE 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-123>

Gestion du document

Référence	CERTA-2004-AVI-123-003
Titre	Vulnérabilité du service IKE racoon
Date de la première version	08 avril 2004
Date de la dernière version	13 mai 2004
Source(s)	Bulletin de sécurité GLSA-200404-05 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

Usurpation d'identité.

2 Systèmes affectés

Paquetage IPsec-tools (pour les noyaux linux 2.6) version 0.3rc4 et antérieures.

3 Résumé

Une vulnérabilité est présente dans le service racoon lors de l'authentification en phase 1 basée sur des certificats X.509.

4 Description

racoon est un service de gestion des clefs IKE. racoon gère notamment les associations de sécurité (SA ou Security Association) pour du trafic réseau chiffré et/ou authentifié (IPSEC).

Une vulnérabilité est présente dans `racoon` dans le cas où les certificats X.509 sont utilisés pour l'authentification en phase 1. `racoon` ne vérifiant pas les signatures RSA, il est possible pour un utilisateur mal intentionné de réaliser une usurpation d'identité.

5 Solution

- La version 0.3rc5 du paquetage `ipsec-tools` corrige cette vulnérabilité :
<http://ipsec-tools.sourceforge.net>
- Bulletin de sécurité GLSA-200404-05 de Gentoo
<http://www.gentoo.org/security/en/glsa/glsa-200404-05.xml>
- Bulletin de sécurité MDKSA-2004:027 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:027>

6 Documentation

- Projet Kame :
<http://www.kame.net>
- Message de Ralf Spennberg "CAN-2004-0155: The KAME IKE daemon racoon":
<http://marc.theaimsgroup.com/?l=full-disclosure&m=108137769100111&w=2>
- Avis de sécurité FreeBSD du 07 avril 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD `racoon` :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Bulletin de sécurité RedHat RHSA-2004-165 du 11 mai 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-165.html>
- Référence CVE CAN-2004-0155 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0155>

Gestion détaillée du document

08 avril 2004 version initiale.

13 avril 2004 ajout référence au bulletin de sécurité de Mandrake.

12 mai 2004 ajout références aux bulletins de sécurité FreeBSD et NetBSD.

13 mai 2004 ajout référence au bulletin de sécurité RedHat.