Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2008
N° CERTA-2008-AVI-056-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la pile IPv6 du projet KAME

Gestion du document

Référence	CERTA-2008-AVI-056-001
Titre	Vulnérabilité dans la pile IPv6 du projet KAME
Date de la première version	07 février 2008
Date de la dernière version	14 février 2008
Source(s)	Note de vulnérabilité VU110947 de l'US-CERT du 06 février 2008
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Tous les systèmes mettant en œuvre la pile protocolaire IPv6 du projet KAME.

La note de vulnérabilité VU110947 de l'US-CERT du 06 février 2008 liste les différents systèmes, ainsi que les dates de leur mise à jour.

3 Résumé

Une vulnérabilité a été identifiée dans la mise en œuvre d'IPv6 par le projet KAME. L'exploitation de celle-ci permet à une personne distante malveillante de perturber le fonctionnement du système via un paquet spécialement construit.

4 Description

Une vulnérabilité a été identifiée dans la mise en œuvre d'IPv6 par le projet KAME. La pile ne manipulerait pas correctement les trames utilisant l'en-tête `IPComp` dans le fichier `ipcomp_input.c`. Celui-ci est défini par le standard RFC 3173 et précise un protocole de compression sans perte des données dans un datagramme IP.

L'exploitation de cette vulnérabilité permet à une personne distante malveillante de perturber le fonctionnement du système via un paquet spécialement construit.

Plusieurs systèmes s'appuient sur la mise en œuvre du projet KAME.

5 Solution

Se référer au bulletins de sécurités des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Correctif de NetBSD concernant la vulnérabilité `ipcomp_input.c` :
  http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/netinet6/ipcomp_input.c?f=u&only_with_tag=netbsd-3-1
- Bulletin de sécurité FreeBSD-SA-08:04.ipsec.asc :
  http://security.freebsd.org/advisories/FreeBSD-SA-08:04.ipsec.asc
- Note de vulnérabilité de l'US-CERT VU#110947 du 06 février 2008 :
  http://www.kb.cert.org/vuls/id/110947
- Référence CVE CVE-2008-0177 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0177
- Standard IETF RFC 3173, "IP Payload Compression Protocol (IPComp)", septembre 2001 :
  http://www.ietf.org/rfc/rfc3173.txt
- Aperçu du projet KAME concernant la mise en œuvre IPv6 :
  http://www.kame.net/project-overview.html

Gestion détaillée du document

07 février 2008 version initiale.

14 février 2008 ajout de la référence au bulletin de FreeBSD.