

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ISAKMPD sous OpenBSD

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-399>

Gestion du document

Référence	CERTA-2004-AVI-399
Titre	Vulnérabilité dans ISAKMPD sous OpenBSD
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Correctif de sécurité OpenBSD du 14 décembre 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

OpenBSD versions 3.4, 3.5 et 3.6.

3 Description

`isakmpd` est un service basé sur le protocole IKE. `isakmpd` sert notamment à la négociation et à la gestion des associations de sécurité (SA) pour du trafic réseau chiffré et/ou authentifié (IPSEC).

Une vulnérabilité a été découverte dans le service `isakmpd` lors de son utilisation avec le protocole IPSEC.

Un utilisateur local mal intentionné peut exploiter cette vulnérabilité afin de créer un déni de service.

4 Solution

Appliquer le correctif suivant la version affectée :

– OpenBSD version 3.4 :

- ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/035_pfkey.patch
- OpenBSD version 3.5 :
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/024_pfkey.patch
- OpenBSD version 3.6 :
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/007_pfkey.patch

5 Documentation

Bulletin de sécurité OpenBSD #007 du 14 décembre 2004 :
<http://www.openbsd.org/errata.html#pfkey>

Gestion détaillée du document

15 décembre 2004 version initiale.