

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de 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-100>

---

### Gestion du document

Référence	CERTA-2004-AVI-100-001
Titre	Multiples vulnérabilités de isakmpd sous OpenBSD
Date de la première version	24 mars 2004
Date de la dernière version	12 mai 2004
Source(s)	Bulletin de sécurité R7-0018 de Rapid7
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 3.4 et versions antérieures ;
- OpenBSD-current du 17 mars 2004 et versions antérieures.

## 3 Résumé

De multiples vulnérabilités présentes dans le service `isakmpd` peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service sur la plate-forme vulnérable.

## 4 Description

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

Au moyen de paquets habilement constitués, un utilisateur mal intentionné peut réaliser un déni de service par arrêt intempestif du service ou consommation excessive des ressources du systèmes (mémoire, CPU).

## 5 Solution

Pour OpenBSD version 3.4, appliquer le correctif disponible à cette adresse :  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/015\\_isakmpd2.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/015_isakmpd2.patch)  
Pour OpenBSD version 3.3, appliquer le correctif disponible à cette adresse :  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.3/common/020\\_isakmpd2.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.3/common/020_isakmpd2.patch)

## 6 Documentation

- Bulletin de sécurité R7-0018 de Rapid7 :  
<http://www.rapid7.com/advisories/R7-0018.html>
- Bulletin de sécurité OpenBSD #015 du 17 mars 2004 :  
<http://www.openbsd.org/errata.html#isakmpd2>
- Avis de sécurité FreeBSD du 31 mars 2004 :  
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD isakmpd :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2004-0218 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0218>
- Référence CVE CAN-2004-0219 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0219>
- Référence CVE CAN-2004-0220 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0220>
- Référence CVE CAN-2004-0221 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0221>
- Référence CVE CAN-2004-0222 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0222>

## Gestion détaillée du document

**24 mars 2004** version initiale.

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