

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du service vpnd de VPN-1/Firewall-1

---

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-2005-AVI-459>

---

### Gestion du document

Référence	CERTA-2005-AVI-459
Titre	Vulnérabilité du service vpnd de VPN-1/Firewall-1
Date de la première version	16 novembre 2005
Date de la dernière version	–
Source(s)	Avis de sécurité 273756/NISCC/ISAKMP de l'UNIRAS
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 distant.

## 2 Systèmes affectés

- VPN-1/Firewall-1 NG AI R54, R55, R55W, R55P,
- VPN-1 Pro NGX R60,
- Check Point Express CI R57,
- Firewall-1 GX 3.0.

## 3 Résumé

Un utilisateur distant mal intentionné peut initier une négociation IKE volontairement mal formée qui va provoquer l'arrêt du service concerné, vpnd.

## 4 Description

IKE est un protocole utilisé pour la négociation des associations de sécurité pour IPsec. Une erreur dans le code de vpnd le rend vulnérable à une attaque en déni de service.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Bulletin de sécurité CheckPoint sk31316 du 16 novembre 2005 :  
<http://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31316>
- Avis de sécurité de l'UNIRAS 273756/NISCC/ISAKMP du 14 novembre 2005 :  
<http://www.uniras.gov.uk/niscc/docs/br-20051114-01013.html>

## **Gestion détaillée du document**

**16 novembre 2005** version initiale.