

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité ISAKMP dans Checkpoint VPN-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-2004-AVI-155>

---

## Gestion du document

Référence	CERTA-2004-AVI-155
Titre	Vulnérabilité ISAKMP dans Checkpoint VPN-1
Date de la première version	05 mai 2004
Date de la dernière version	–
Source(s)	Alerte Checkpoint du 04 mai 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

Exécution de code arbitraire.

## 2 Systèmes affectés

- VPN-1/Firewall-1 NG avec l'application Intelligence R55 ;
- VPN-1/Firewall-1 NG avec l'application Intelligence R54 HFA-410 ;
- VPN-1/Firewall-1 NG FP3 HFA-325 ;
- VPN-1/Firewall-1 VSX ;
- VPN-1/Firewall-1 VSX NG avec l'application Intelligence ;
- VPN-1/Firewall-1 GX ;
- VPN-1 SecuRemote/SecureClient NG avec l'application Intelligence R56.

## 3 Résumé

Une vulnérabilité a été découverte dans la mise en œuvre du protocole ISAKMP dans Checkpoint VPN-1.

## **4 Description**

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est un protocole d'initialisation de communication utilisé par le protocole IPSEC. Une vulnérabilité est présente dans la mise en œuvre du protocole ISAKMP dans Checkpoint VPN-1 qui permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance lors de la négociation d'un tunnel VPN. Cette vulnérabilité n'affecte pas les utilisateurs n'utilisant pas de solution VPN ou ayant une version mise à jour pour VPN-1 Firewall-1 R55 HFA-03, R54 HFA-410, NG FP3 HFA-325 ou VPN-1 SecuRemote/SecureClient R56.

## **5 Solution**

Appliquer le correctif suivant la version affectée (cf. Documentation).

## **6 Documentation**

Alerte de sécurité Checkpoint du 04 Mai 2004 :  
[http://www.checkpoint.com/techsupport/alerts/ike\\_vpn.html](http://www.checkpoint.com/techsupport/alerts/ike_vpn.html)

## **Gestion détaillée du document**

**05 mai 2004** version initiale.