

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Check Point Connectra

---

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-2007-AVI-043>

---

### Gestion du document

Référence	CERTA-2007-AVI-043
Titre	Vulnérabilité de Check Point Connectra
Date de la première version	22 janvier 2007
Date de la dernière version	–
Source(s)	Mise à jour Check Point du 22 janvier 2007
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

– Check Point Connectra R62 ainsi que des versions antérieures.

## 3 Description

Une vulnérabilité a été identifiée dans Check Point Connectra, une solution de passerelle permettant de déployer et contrôler les accès SSL VPN. Des fichiers de session ne seraient pas correctement vérifiés. Une personne malveillante pourrait donc exploiter cette vulnérabilité pour contourner la politique de sécurité et connecter une machine compromise au réseau, sans que celle-ci subisse de tests préalables. Ces tests font cependant partie de la solution Check Point, nommée *Comprehensive endpoint security*.

## 4 Solution

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

## **5 Documentation**

- Mise à jour de sécurité Check Point du 22 janvier 2007 :  
<http://www.checkpoint.com/downloads/>
- Référence CVE CVE-2007-0471 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0471>

### **Gestion détaillée du document**

**22 janvier 2007** version initiale.