

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans des produits Check Point ZoneAlarm

---

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-186>

---

### Gestion du document

Référence	CERTA-2007-AVI-186
Titre	Vulnérabilités dans des produits Check Point ZoneAlarm
Date de la première version	24 avril 2007
Date de la dernière version	–
Source(s)	Avis de sécurité iDefense 517 du 20 avril 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 ;
- élévation de privilèges.

## 2 Systèmes affectés

- les produits ayant une version du ZoneAlarm Spyware Removal Engine (SRE) antérieure à la 5.0.156.0.

## 3 Description

Des vulnérabilités ont été identifiées dans certains produits de sécurité Check Point ZoneAlarm, et plus précisément dans le pilote `srescan.sys` qui gère entre autres des mesures de désinfection (SRE, pour Spyware Removal Engine).

Le pilote ne vérifierait pas correctement certaines adresses qui lui sont communiquées, ce qui pourrait être exploité pour accéder à des zones arbitraires de la mémoire. Une personne malveillante pourrait ainsi élever ses privilèges à ceux du SYSTEM.

## **4 Solution**

Se référer aux mises à jour de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **5 Documentation**

- Bulletin de sécurité iDefense 517 du 20 avril 2007 :  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=517>
- Site de Check Point ZoneAlarm pour accéder aux mises à jour :  
<http://www.zonealarm.com/store/content/home.jsp?lang=fr&ctry=FR&dc=34std>

## **Gestion détaillée du document**

**24 avril 2007** version initiale.