

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans des produits Check Point

---

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-282>

---

### Gestion du document

Référence	CERTA-2007-AVI-282
Titre	Vulnérabilités dans des produits Check Point
Date de la première version	28 juin 2007
Date de la dernière version	–
Source(s)	Avis de sécurité de Calyptix CX-2007-04 du 26 juin 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 Safe@Office Appliances 7.x ;
- Check Point VPN-1 UTM Edge ;
- Check Point ZoneAlarm Z100G 7.x.

Les versions du logiciel antérieures à 7.0.45 seraient affectées.

## 3 Description

Une vulnérabilité de type injection de code indirecte serait possible : une personne malveillante pourrait exécuter du code arbitraire sur le système par le biais d'une page Web spécialement construite, et à la condition que l'utilisateur légitime soit connecté à la fois sur cette page et sur l'interface du système.

Une seconde vulnérabilité permettrait à tout utilisateur connecté au système de modifier le mot de passe de l'administrateur, sans connaître celui existant.

## 4 Solution

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

## 5 Documentation

- Avis de sécurité Calyptix CX-2007-04 du 26 juin 2007 :  
<http://labs.calyptix.com/CX-2007-04.php>
- Mises à jour disponibles de Check Point :  
<http://www.sofaware.com/supportDownloads.aspx?boneId=182>
- Site officiel de Check Point :  
<http://www.checkpoint.com>
- Référence CVE CVE-2007-3462 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3462>

## Gestion détaillée du document

**28 juin 2007** version initiale.