

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2013-AVI-487>

Gestion du document

Référence	CERTA-2013-AVI-487
Titre	Vulnérabilité dans Check Point
Date de la première version	22 août 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Check Point du 21 août 2013
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(s)

- déni de service à distance
- contournement de la politique de sécurité

2 Systèmes affectés

- Check Point R75.X sous Gaia OS
- Check Point R76 sous Gaia OS
- Check Point R75.X sous IPSO 6.2 OS
- Check Point R76 sous IPSO 6.2 OS

3 Résumé

Une vulnérabilité a été corrigée dans *Check Point*. Elle permet à un attaquant de provoquer un déni de service à distance et un contournement de la politique de sécurité.

4 Solution

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

5 Documentation

– Bulletin de sécurité Check Point du 21 août 2013

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk94490

Gestion détaillée du document

22 août 2013 version initiale.