

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les 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-2009-AVI-376>

Gestion du document

Référence	CERTA-2009-AVI-376
Titre	Vulnérabilité dans les produits Check Point
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Check Point sk42723 et 42725 du 08 septembre 2009
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

Déni de service à distance.

2 Systèmes affectés

- Check Point VPN-1 Power/UTM ;
- Check Point Connectra ;
- Check Point IPSO ;
- Check Point VPN-1 Power VSX ;
- Check Point Integrity ;
- Check Point UTM-1 Edge ;
- Check Point IPS-1 ;
- Check Point Security Management ;
- Check Point SmartCenter.

3 Résumé

Une vulnérabilité présente dans les équipements Check Point permet à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Une vulnérabilité est présente dans la mise en œuvre du protocole TCP sur les équipements Check Point. Cette faille permet à un utilisateur distant malintentionné de provoquer un déni de service de l'équipement vulnérable au moyen de paquets TCP / IP construits de façon particulière.

5 Solution

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

6 Documentation

- Bulletins de sécurité Check Point sk42723 et sk 42725 du 08 septembre 2009 :
<http://supportcontent.checkpoint.com/solutions?id=42723>
<http://supportcontent.checkpoint.com/solutions?id=42725>
- Référence CVE CVE-2008-4609 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609>

Gestion détaillée du document

09 septembre 2009 version initiale.