

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Check Point VPN-1

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-004>

Gestion du document

Référence	CERTA-2009-AVI-004
Titre	Vulnérabilité dans Check Point VPN-1
Date de la première version	07 janvier 2009
Date de la dernière version	–
Source(s)	Réponse Check Point sk36321 du 28 décembre 2008
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 VPN-1 R65 sans mise à jour HFA_30.

3 Résumé

Une vulnérabilité a été identifiée dans Check Point VPN-1. Elle permet à une personne distante malveillante de récupérer des informations sur l'adressage réseau interne.

4 Description

Une vulnérabilité a été identifiée dans le pare-feu Check Point VPN-1 configuré pour faire de la traduction de port (PAT). Une personne malveillante distante peut émettre certaines trames à destination du port public traduit et récupérer en retour des messages d'erreurs ICMP fournissant des informations IP incorrectement nettoyées. Cela permet d'obtenir des informations sur l'adressage IP interne.

5 Solution

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

6 Documentation

- Réponse de sécurité CheckPoint sk36321 du 28 décembre 2008 :
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk36321
- Référence CVE CVE-2008-5849 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5849>
- Avis de sécurité Portcullis 08-009 du 14 novembre 2009 :
<http://www.portcullis-security.com/293.php>

Gestion détaillée du document

07 janvier 2009 version initiale.