

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Checkpoint 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-2008-AVI-149>

Gestion du document

Référence	CERTA-2008-AVI-149
Titre	Vulnérabilité dans Checkpoint VPN-1
Date de la première version	19 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Checkpoint sk34579 du 18 mars 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

- Déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- VPN-1 Power / UTM NGX R65 ;
- VPN-1 Pro NGX R62 GA ;
- VPN-1 Pro NGX R61 ;
- VPN-1 Pro NGX R60 ;
- VPN-1 / Firewall-1 NG with AI R55 ;
- VPN-1 Power / UTM NGX R65 with Messaging Security.

3 Résumé

Une vulnérabilité dans Checkpoint VPN-1 permet à une personne malintentionnée de causer un déni de service à distance et/ou de porter atteinte à la confidentialité des données.

4 Description

Une vulnérabilité permettant à une personne malveillante de cause un déni de service à distance et/ou de porter atteinte à la confidentialité des données a été découverte dans Checkpoint VPN-1. Cette faille concerne le scénario suivant :

- deux passerelles A et B sont connectées et forment un tunnel VPN ;
- une machine C se connecte à la passerelle A. Elle a une IP qui est également définie dans le domaine de chiffrement de la passerelle B, ce qui cause des collisions ;
- les nouvelles connexions destinées à l'IP du domaine de chiffrement seront alors transférées à la machine C.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs ou des changements à apporter dans la configuration (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Checkpoint sk34579 du 18 mars 2008 :
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34579

Gestion détaillée du document

19 mars 2008 version initiale.