Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 13 juillet 2001
N° CERTA-2001-AVI-075

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Firewall-1

Gestion du document

Référence	CERTA-2001-AVI-075
Titre	Vulnérabilité de Firewall-1
Date de la première version	13 juillet 2001
Date de la dernière version	–
Source(s) Avis CA-2001-17 du CERT/CC	Avis de Checkpoint 2001-07-09
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 des règles de sécurité.

2 Systèmes affectés

CheckPoint Firewall-1 et VPN-1 version 4.1.

3 Résumé

Le port 259/UDP n'est pas correctement bloqué par Firewall-1.

4 Description

RDP de CheckPoint est un protocole propriétaire différent du protocole RDP (*Reliable Data Protocol* décrit par la RFC 908). Le port 259/UDP de Firewall-1, permet d'envoyer des commandes simples RDP chiffrées au garde barrière.

Malheureusement, une mauvaise implémentation des règles de sécurité du logiciel, permet à des paquets UDP de traverser le port 259 du garde barrière dans n'importe quel sens sans être bloqué par ce dernier.

5 Contournement provisoire

Filtrer le port 259/UDP sur les routeurs de périphérie.

6 Solution

Appliquer le correctif de CheckPoint après avoir installé le *Service Pack 4* :
http://www.checkpoint.com/techsupport/downloads.html
Et installer à nouveau les règles de sécurité.

7 Documentation

L'avis de sécurité de Checkpoint :
http://www.checkpoint.com/techsupport/alerts/rdp.html

Gestion détaillée du document

13 juillet 2001 version initiale.