

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités sous Firewall-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-2000-AVI-022>

---

### Gestion du document

Référence	CERTA-2000-AVI-022
Titre	Vulnérabilités sous Firewall-1
Date de la première version	03 août 2000
Date de la dernière version	–
Source(s)	réseau de confiance Avis du CERT IST
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 via le protocole SMTP ;
- déni de service par fragmentation IP ;
- contournement du contrôle des connexions unidirectionnelles ;
- contournement des règles de sécurités par rsh/rexec ;
- détournement de connexion FTP ;
- détournement de paquets encapsulés ;
- contournement des mécanismes d'authentification ;
- arrêt du garde-barrière.

## 2 Systèmes affectés

CheckPoint Firewall-1 version 4.1

## 3 Résumé

De nombreuses vulnérabilités de Firewall-1 ont été publiées récemment.

## 4 Description

La liste des vulnérabilités de Firewall-1 corrigées par le Service Pack 2 est la suivante :

- Une salve rapide de commandes SMTP envoyée au serveur de sécurité pour SMTP peut faire monter la charge du processeur jusqu'au blocage complet du transfert du courrier. Cependant, le reste du trafic continue de fonctionner normalement.
- Les mécanismes utilisés pour tenir un historique des paquets fragmentés lors d'une attaque consomment une grosse charge du processeur et aboutit à un déni de service du garde-barrière.
- Par une malformation de requêtes TCP fragmentées, ou de multiples connexions puis déconnexions successives, il est possible de passer outre les contrôles de connexions unidirectionnelles.
- Des requêtes de connexions RSH/REXEC malformées permettent à un serveur RSH/REXEC externe d'établir une connexion non-autorisée avec un client protégé (interne). Ceci ne peut se produire que si l'administrateur de Firewall-1 y a autorisé les connexions RSH/REXEC).
- Dans certaines conditions, les connexions FTP d'un serveur vers un client peuvent être détournées vers un client non-désiré.
- Des paquets encapsulés FWZ (chiffrés) peuvent passer normalement les règles du garde-barrière même s'ils ne proviennent pas d'un de ses clients.
- Les mécanismes d'authentications des communications inter-modules sont attaquables et permettent un déni de service du garde-barrière.
- Les mécanismes d'authentification utilisés par OPSEC peuvent être sujet à des usurpations d'identité.
- Les mécanismes d'authentification inter-module utilisés dans l'authentification par challenge-réponse pour les versions 3.1 et 4.0 du logiciel sans réseau privé virtuel (*non-VPN software*) est attaquable, en tentant toutes les possibilités.
- Une mauvaise implémentation du protocole de communication inter-module peut-être exploité pour effectuer un dépassement de mémoire dans Getkey. Ceci a pour conséquence l'arrêt du daemon de FIREWALL-1.

## 5 Contournement provisoire

Bien que la majorité de ces vulnérabilités puissent être évitées par un renforcement des règles du Firewall, il est obligatoire d'appliquer le correctif au plus vite.

## 6 Solution

Appliquer le Service Pack 2 disponible sur le site de CheckPoint à l'adresse :

<http://www.checkpoint.com/sp>

ou :

<http://www.checkpoint.com/cgi-bin/download.cgi>

## 7 Documentation

Avis de CheckPoint au sujet de ces vulnérabilités :

[http://www.checkpoint.com/techsupport/alerts/list\\_vun.html](http://www.checkpoint.com/techsupport/alerts/list_vun.html)

Conseil de mise à jour en fonction de l'installation :

<http://www.securitywatch.com/scripts/news/list.asp?AID3462>

## Gestion détaillée du document

03 août 2000 version initiale.