

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de « Fast Mode » 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-091>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2000-AVI-091 |
| Titre | Vulnérabilité de « Fast Mode » sous Firewall-1 |
| Date de la première version | 20 décembre 2000 |
| Date de la dernière version | – |
| Source(s) | CheckPoint |
| 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 VPN-1/Firewall-1 4.1 et 4.0

3 Résumé

« Fast Mode » est un mode permettant d'améliorer les performances de FireWall-1 vis-à-vis du protocole TCP/IP.

Une vulnérabilité de ce mode de fonctionnement permet à un utilisateur mal intentionné d'avoir accès à des services qui sont normalement interdits par le garde barrière.

4 description

Une erreur dans *Fast Mode* rend vulnérable une machine et tout le réseau qui l'entoure lorsque l'on ouvre l'accès à un des services de celle-ci. En effet : lorsqu'on modifie les règles du garde-barrière afin d'ouvrir l'accès à un service sur une machine, le garde-barrière permet l'accès à tous les services auxquels « Fast Mode » est appliqué pour cette machine et pour celles qui se situent dans le même sous-réseau qu'elle.

5 Contournement provisoire

Désactiver *Fast Mode* sur le garde barrière.

Note : l'option *Fast Mode* n'est pas activée sur le garde-barrière par défaut.

6 Solution

Appliquer le *Service Pack* (SP) qui convient à votre garde-barrière.

- SP3 pour la version 4.1 ;
- SP8 pour la version 4.0.

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

7 Documentation

Avis de sécurité de Checkpoint :

<http://www.checkpoint.com/techsupport/alerts/fastmode.html>

Gestion détaillée du document

20 décembre 2000 version initiale.