

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans le garde-barrière Firewall-1 NG

---

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-2003-AVI-056>

---

### Gestion du document

Référence	CERTA-2003-AVI-056
Titre	Vulnérabilités dans le garde-barrière Firewall-1 NG
Date de la première version	24 mars 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Checkpoint Firewall-1 NG FP3.

## 3 Résumé

Le garde-barrière Checkpoint Firewall-1 NG FP3 possède un démon `syslog` permettant la consolidation de journaux provenant de plusieurs matériels. Celui-ci présente plusieurs vulnérabilités.

## 4 Description

L'envoi de caractères malicieux vers le démon `syslog` entraîne une consommation excessive du temps CPU. Cette vulnérabilité peut être exploitée par un individu mal intentionné afin d'effectuer un déni de service sur le garde-barrière.

Un utilitaire en ligne de commande (`fw log -nfnl`) présent dans le garde-barrière permet la visualisation de messages des journaux `syslog` sur une console. Une vulnérabilité présente dans cet utilitaire permet à un individu mal intentionné d'injecter des caractères malicieux afin d'en fausser l'affichage.

## 5 Contournement provisoire

Filtrer le port 514/UDP pour n'accepter des paquets provenant uniquement de sources sûres.

## 6 Solution

La première vulnérabilité peut être corrigée par l'application du correctif HF2 (cf. Documentation ) ou bien par l'utilisation de l'outil `SmartUpdate`.

Aucun correctif n'est disponible pour la seconde vulnérabilité le jour de la rédaction de l'avis. Il est toutefois recommandé de ne pas utiliser cet utilitaire afin de visualiser les messages `syslog` ou de filtrer les caractères non désirés.

## 7 Documentation

Bulletin de sécurité Checkpoint :

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

Bulletin de sécurité AERASEC :

<http://www.aerasesc.de/security/advisories/checkpoint-fw1-ng-fp3-syslog-crash.txt>

## Gestion détaillée du document

24 mars 2003 version initiale.