Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 février 2004
N° CERTA-2004-AVI-022

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du garde-barrière Firewall-1

Gestion du document

Référence	CERTA-2004-AVI-022
Titre	Vulnérabilité du garde-barrière Firewall-1
Date de la première version	05 février 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité "Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities" d'ISS
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

- Firewall-1 NG avec Application Intelligence (AI) R55 et R54 ;
- Firewall-1 NG FP3 et versions antérieures avec HTTP Security Server.

3 Résumé

Une vulnerabilité présente dans le composant réalisant le filtrage des requêtes HTTP au niveau du garde-barrière Check Point Firewall-1 peut être exploitée à distance par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

Une vulnérabilité de type chaîne de format est présente au niveau du serveur mandataire (`proxy`) HTTP du garde-barrière Firewall-1.

Au moyen de requêtes HTTP habilement constituées, un utilisateur distant mal intentionné peut exécuter du code arbitraire sur le garde-barrière vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Bulletin de sécurité "Firewall-1 HTTP Security Server Vulnerability" de Check Point :
  http://www.checkpoint.com/techsupport/alerts/securityserver.html
- Bulletin de sécurité "Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities" d'Internet Security Systems :
  http://xforce.iss.net/xforce/alerts/id/162
- Référence CVE CAN-2004-0039 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0039

Gestion détaillée du document

05 février 2004 version initiale.