Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 août 2003
N° CERTA-2003-AVI-131

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur les gardes-barrières NetScreen

Gestion du document

Référence	CERTA-2003-AVI-131
Titre	Vulnérabilité sur les gardes-barrières NetScreen
Date de la première version	01 août 2003
Date de la dernière version	–
Source(s)	Avis de sécurité 57739 de NetScreen
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.

2 Systèmes affectés

Les gardes barrières et VPN NetScreen sous ScreenOS
- versions 4.0.1r1 à 4.0.1r6 ;
- version 4.0.3r1 ;
- version 4.0.3r2.

3 Résumé

Une vulnérabilité sur les gardes-barrières et VPN NetScreen permet à un utilisateur mal intentionné, via un paquet malicieusement construit, de réaliser un déni de service du garde barrière.

4 Description

Il est possible d'administrer les gardes-barrières NetScreen par différentes méthodes : `telnet, WebAuth (http / https), ssh,` ou `ProxyAuth`.

Un utilisateur mal intentionné non privilègié peut, en utilisant les protocoles `telnet, http` ou `https`, réaliser un déni de service du garde-barrière par l'envoi, d'un paquet malicieusement construit adressé à celui-ci.

5 Contournement provisoire

- Activer la caractéristique « anti-spoofing » sur le garde barrière.
- Utiliser le protocole `ssh` plutôt que le protocole `telnet`.
- Utiliser l'authentification par `ProxyAuth`.

6 Solution

Appliquer les correctifs correspondant à votre version (cf. section documentation).

7 Documentation

- Avis de sécurité 57739 de NetScreen :
  http://www.netscreen.com/services/security/alerts/advisory-57739.txt
- Correctif de NetScreen :
  http://www.netscreen.com/services/download_soft/

Gestion détaillée du document

01 août 2003 version initiale.