



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 juillet 2004  
N° CERTA-2004-AVI-227

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les pare-feux NetScreen 5GT

---

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-2004-AVI-227>

---

### Gestion du document

Référence	CERTA-2004-AVI-227
Titre	Vulnérabilité dans les pare-feux NetScreen 5GT
Date de la première version	06 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper du 29 juin 2004
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

Vol d'informations.

## 2 Systèmes affectés

Juniper Networks NetScreen 5GT possédant un antivirus (AV).

## 3 Description

Une vulnérabilité de type `cross site scripting` est présente dans le moteur antivirus disponible avec les pare-feux NetScreen 5GT. Un utilisateur mal intentionné peut exploiter cette faille afin de récupérer de l'information sur les postes protégés par le pare-feu à l'aide d'un fichier compressé contenant un virus et possédant un nom malicieusement formé.

## 4 Solution

Mettre à jour la version de ScreenOS (cf. Documentation).

## **5 Documentation**

- Bulletin de sécurité Juniper du 29 juin 2004 :  
<http://juniper.net/support/security/alerts/screenos-av-xss-2.txt>
- Note d'information CERTA-2002-INF-001 du CERTA sur le cross site scripting :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/>

### **Gestion détaillée du document**

**06 juillet 2004** version initiale.