



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2003
N° CERTA-2003-AVI-108

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ScreenOS

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-108>

Gestion du document

Référence	CERTA-2003-AVI-108
Titre	Vulnérabilité dans ScreenOS
Date de la première version	15 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #57605 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les équipements possédant une version 4.0.3 ou antérieure de ScreenOS et fonctionnant en mode transparent.

3 Résumé

Une vulnérabilité présente dans ScreenOs permet à un individu mal intentionné d'effectuer des dénis de service ou de contourner la politique de sécurité lorsque le pare-feu est configuré en mode transparent.

4 Description

Le mode transparent est un mode activé par défaut sur certains pare-feu NetScreen. L'activation de ce mode permet d'utiliser le pare-feu de manière transparente comme un pont.

Un individu mal intentionné situé dans le même domaine de diffusion que le pare-feu peut injecter certains paquets non-IP afin de contourner la politique de sécurité mise en place ou d'effectuer des dénis de service.

5 Solution

Appliquer les correctifs fournis par le constructeur (cf. Documentation).

6 Documentation

Bulletin de sécurité #57605 de NetScreen :

<http://www.netscreen.com/services/security/alerts/advisory-57605.txt>

Révision du bulletin de sécurité #57605 de NetScreen :

<http://www.netscreen.com/services/security/alerts/57605-correction.txt>

Gestion détaillée du document

15 juillet 2003 version initiale.