

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les pare-feux Netscreen

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-2002-AVI-257>

Gestion du document

Référence	CERTA-2002-AVI-257
Titre	Multiples vulnérabilités dans les pare-feux Netscreen
Date de la première version	02 décembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité 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

- Contournement du mécanisme de blocage des URLs ;
- contournement des règles de sécurité du pare-feu ;
- déni de service.

2 Systèmes affectés

Pare-feux Netscreen avec ScreenOS 1.7, 2.6, 2.7.1, 2.8, 3.0, 3.1, 4.0.

3 Résumé

De multiples vulnérabilités des gardes-barrières Netscreen permettent de contourner divers mécanismes de sécurité ou de réaliser un déni de service.

4 Description

Trois vulnérabilités affectent les pare-feux Netscreen :

- Vulnérabilité de la fonctionnalité Malicious-URLs :

La fonctionnalité Malicious-URLs permet de bloquer l'accès à certains sites HTTP externes. Il est possible de contourner le mécanisme de blocage en fragmentant l'en-tête HTTP.

- Vulnérabilité des numéros de séquence TCP :

Les numéros de séquence TCP (ISN TCP) des pare-feux Netscreen sont prévisibles. En exploitant cette vulnérabilité, et en la combinant à l'usurpation d'adresse IP, il est possible de contourner certaines règles de sécurité.

- Vulnérabilité dans le contrôle des sessions H.323 :

Les sessions H.323 semi-ouvertes ne sont pas purgées assez régulièrement. En exploitant cette vulnérabilité, un utilisateur mal intentionné peut saturer les entrées de la table de sessions.

5 Solution

Appliquer le correctif de Netscreen selon la version de ScreenOS, ou bien passer en version 4.0.1.

Consulter le site de Netscreen pour connaître la disponibilité des correctifs.

Les correctifs peuvent être téléchargés à l'adresse suivante :

<http://www.netscreen.com/support/updates.html>

6 Documentation

Avis de sécurité 51929 de Netscreen :

http://www.netscreen.com/support/alerts/malicious_URL.html

Avis de sécurité 51897 de Netscreen :

http://www.netscreen.com/support/alerts/Predictable_TCP_Initial_Sequence_Numbers.html

Avis de sécurité 52020 de Netscreen :

http://www.netscreen.com/support/alerts/Potential_H_323_Denial_of_Service.html

Gestion détaillée du document

02 décembre 2002 version initiale.