

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les équipements NetScreen Firewall/VPN

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-158>

Gestion du document

Référence	CERTA-2003-AVI-158
Titre	Vulnérabilité dans les équipements NetScreen Firewall/VPN
Date de la première version	07 octobre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #57983 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

Fuite d'informations.

2 Systèmes affectés

Les équipements NetScreen Firewall/VPN fonctionnant en tant que serveur DHCP et possédant une version de ScreenOS inférieure à 4.0.3r3.

3 Résumé

Dans certaines conditions, les équipements fonctionnant en tant que serveur DHCP et administrés par HTTP peuvent divulguer des informations sensibles telles que des noms d'utilisateur ou des mots de passe encodés.

4 Description

La réutilisation d'un tampon mémoire précédemment utilisé pour la gestion du contexte d'une session d'administration via HTTP peut entraîner, dans certains cas, la divulgation des informations lors du traitement d'une réponse à une requête DHCP.

5 Solution

Appliquer le correctif suivant la version affectée (cf. Documentation).

6 Documentation

Bulletin de sécurité #57983 de NetScreen :

http://www.netscreen.com/services/security/alerts/10_01_03_57983_v003.jsp

Gestion détaillée du document

07 octobre 2003 version initiale.