Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 mars 2004
N° CERTA-2004-AVI-068

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits VPN NetScreen

Gestion du document

Référence	CERTA-2004-AVI-068
Titre	Vulnérabilité sur les produits VPN NetScreen 5000
Date de la première version	05 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité de NetScreen 58412
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

Elévation de privilèges.

2 Systèmes affectés

NetScreen-SA IVE de la version 3.0 à la version 3.3.1 présent sur les produits VPN NetScreen 5000.

3 Résumé

Une vulnérabilité de type « cross site scripting » a été découverte sur l'interface d'administration des produits VPN NetScreen-SA séries 5000.

4 Description

Une vulnérabilité de type « cross site scripting » sur le script CGI `delhomepage.cgi` de l'interface d'administration des produits VPN NetScreen-SA séries 5000 permet à un utilisateur mal intentionné d'exécuter un script sur le poste client d'un utilisateur authentifié sur ce produit.

5 Solution

Un correctif est disponible sur le site de support de NetScreen (cf. section documentation) pour les sections suivantes :

- 3.2.1 Patch 1-S2
- 3.3-S1
- 3.3 Patch 1-S1
- 3.3.1-S1

6 Documentation

- Avis de sécurité de NetScreen :
  http://www.netscreen.com/services/security/alerts/ive_xss.txt
- Correctifs de NetScreen :
  https://support.neoteris.com
- Note d'information sur les vulnérabilités de type Cross Site Scripting (CERTA-2002-INF-001) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html

Gestion détaillée du document

05 mars 2004 version initiale.