

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des produits d'accès VPN de CheckPoint

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-2011-AVI-251>

Gestion du document

Référence	CERTA-2011-AVI-251
Titre	Vulnérabilité dans des produits d'accès VPN de CheckPoint
Date de la première version	26 avril 2011
Date de la dernière version	–
Source	Bulletin de sécurité CheckPoint sk62410 du 26 avril 2011
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

Injection de code indirecte à distance.

2 Systèmes affectés

- Mobile Access / VPN SSL ;
- SSL Network Extender (SNX).

3 Résumé

Une vulnérabilité dans des produits d'accès en VPN de CheckPoint permet à un utilisateur malveillant d'injecter indirectement du code à distance.

4 Description

Une vulnérabilité existe dans plusieurs produits CheckPoint d'accès en VPN. Lors de l'utilisation au travers d'un navigateur, il est possible à un utilisateur malveillant de faire exécuter du code sur la machine cliente.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité CheckPoint sk62410 du 26 avril 2011 :
<https://supportcenter.checkpoint.com/supportcenter/portal?solutionid=sk62410>
- Référence CVE CVE-2011-1827 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1827>

Gestion détaillée du document

26 avril 2011 version initiale.