

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Check Point SNX, EPS et EPC

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-154>

Gestion du document

Référence	CERTA-2011-AVI-154
Titre	Vulnérabilité dans Check Point SNX, EPS et EPC
Date de la première version	15 mars 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Check Point sk60510 du 24 janvier 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

Élévation de privilèges.

2 Systèmes affectés

Check Point toutes versions de SSL Network Extender (SNX), Endpoint Security Client (EPS) et Endpoint Connect (EPC) sur plateforme Windows sauf :

- EPS R80 ;
- EPS R73 HFA01 ;
- EPC R73 HFA01 ;
- EPS R75 VPN ;
- SNX R75 ;
- SNX R71.30.

3 Résumé

Une vulnérabilité dans les produits Check Point SNX, EPS et EPC permet à un utilisateur malintentionné d'élever ses privilèges sur le système.

4 Description

Une vulnérabilité dans les produits Check Point SNX, EPS et EPC permet à un utilisateur malintentionné, ayant des privilèges d'administration sur les logiciels précédents, d'obtenir les droits de l'utilisateur *LOCAL SYSTEM*.

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 sk60510 du 14 janvier 2011 :
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_docGoviewsolutiondetails=&solutionid=sk60510

Gestion détaillée du document

15 mars 2011 version initiale.