



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juin 2012
N° CERTA-2012-AVI-318

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Check Point Endpoint Connect

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-2012-AVI-318>

Gestion du document

Référence	CERTA-2012-AVI-318
Titre	Vulnérabilité dans Check Point Endpoint Connect
Date de la première version	12 juin 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Check Point du 10 juin 2012
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Check Point Endpoint Security VPN R75 ;
- Check Point Endpoint Security R73.x/E80.x ;
- Check Point Endpoint Connect R73.x ;
- Check Point Remote Access Clients E75.x.

3 Résumé

Une vulnérabilité a été corrigée dans *Check Point Endpoint Connect*. Cette vulnérabilité est due à un chargement de bibliothèque non sécurisé et peut être exploitée pour exécuter du code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité CheckPoint fichier du 10 juin 2012 :
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk76480&src=securityAlerts
- Référence CVE CVE-2012-2753 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2753>

Gestion détaillée du document

12 juin 2012 version initiale.