

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Checkpoint SecureClient

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-2008-AVI-064>

Gestion du document

Référence	CERTA-2008-AVI-064
Titre	Vulnérabilité dans Checkpoint SecureClient
Date de la première version	08 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Checkpoint sk34315 du 06 février 2008
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- VPN-1 SecuRemote / SecureClient NGX R60 pour Windows ;
- VPN-1 SecuRemote / SecureClient NGAI R56 pour Windows.

3 Résumé

Une vulnérabilité dans Checkpoint SecuRemote / SecureClient permet à une personne malintentionnée de contourner la politique de sécurité.

4 Description

Une vulnérabilité a été identifiée dans CheckPoint SecuRemote / SecureClient. La faille consiste en la possibilité de réutiliser de manière triviale les identifiants du VPN. En effet, ceux-ci peuvent être mis en cache dans la base de registre d'un utilisateur et importés sur un autre système. Une personne malintentionnée peut ainsi exploiter cette vulnérabilité pour usurper l'identité d'une personne.

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 sk34315 du 08 février 2008 :
<https://usercenter.checkpoint.com/usercenter/portal/user/anon/page/supportCenter.psml>

Gestion détaillée du document

08 février 2008 version initiale.