Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2004
N° CERTA-2004-AVI-027-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Checkpoint VPN-1

Gestion du document

Référence	CERTA-2004-AVI-027-001
Titre	Vulnérabilité de Checkpoint VPN-1
Date de la première version	09 février 2004
Date de la dernière version	13 février 2004
Source(s)	Avis de sécurité de ISS X-Force du 04 février 2004
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

- Checkpoint VPN-1/FireWall-1 version 4.1 SP5a et versions antérieures ;
- Checkpoint VPN-1/FireWall-1 Next Generation FP0 et FP1.

3 Résumé

Une vulnérabilité dans l'implémentation du protocole ISAKMP par les produits Checkpoint VPN-1 server et Checkpoint VPN SecureRemote/SecureClient permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est un protocole d'initialisation de communications utilisé par le protocole IPSEC. Une vulnérabilité a été découverte dans l'im-

plémentation du protocole `ISAKMP` par les produits Checkpoint VPN-1 server et Checkpoint VPN SecureRemote/SecureClient permettant à un utilisateur mal intentionné d'exécuter du code arbitraire à distance. Aucune authentification n'est nécessaire pour exploiter cette vulnérabilité.

5 Contournement provisoire

Dans l'attente de la mise à jour de vos produits, filtrer le service `ISAKMP` (par défaut 500/UDP).

6 Solution

Contacter l'éditeur pour l'obtention d'un correctif.

7 Documentation

- Bulletin de sécurité de Checkpoint "ISAKMP Alert" du 07 février 2004 :
  http://www.checkpoint.com/techsupport/alerts/41_isakmp.html
- Avis de sécurité de ISS X-Force du 04 février 2004 :
  http://xforce.iss.net/xforce/alerts/id/163
- Avis de sécurité du CERT/CC VU#873334 :
  http://www.kb.cert.org/vuls/id/873334
- Référence CVE CAN-2004-0040 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0040

Gestion détaillée du document

09 février 2004 version initiale.
13 février 2004 correction des systèmes affectés et ajout du bulletin de sécurité de Checkpoint.