



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2004
N° CERTA-2004-AVI-258

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Checkpoint VPN-1 ASN.1

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-2004-AVI-258>

Gestion du document

Référence	CERTA-2004-AVI-258
Titre	Vulnérabilité dans Checkpoint VPN-1 ASN.1
Date de la première version	29 juillet 2004
Date de la dernière version	–
Source(s)	Alerte de sécurité Checkpoint du 28 juillet 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

- Atteinte à la confidentialité des données ;
- exécution de code arbitraire.

2 Systèmes affectés

- VPN-1/FireWall-1 NG avec Application Intelligence R54 et R55 ;
- VPN-1/FireWall-1 NG avec Application Intelligence R55W et R55 ASN.1 ;
- VPN-1/FireWall-1 NG FP3 ASN.1 ;
- VPN-1 SecuRemote/SecuClient NG avec Application Intelligence ;
- Provider-1 NG avec Application Intelligence R54 et R55 ;
- Firewall-1 GX 2.0 et 2.5 ASN.1 ;
- SSL Network Extender ;
- VPN-1/FireWall-1 VSX NG avec Application Intelligence ASN.1 ;
- VPN-1/FireWall-1 VSX 2.0.1 ASN.1.

3 Résumé

Une vulnérabilité a été découverte dans le serveur CheckPoint VPN-1.

4 Description

IKE (Internet Key Exchange) est un système utilisé pour la négociation et l'échange de clés dans l'établissement d'un tunnel chiffré de type VPN. Celui-ci utilise le protocole ISAKMP (Internet Security Association and Key Management Protocol) pour la gestion des clés.

ASN.1 (Abstract Syntax Notation) est un langage standardisé servant à encoder des informations pour la communication entre des systèmes hétérogènes. Il est utilisé par le protocole ISAKMP.

Une vulnérabilité présente dans CheckPoint VPN-1 permet à un utilisateur mal intentionné d'exécuter du code arbitraire lors de l'établissement d'une connexion chiffrée d'un client à un réseau privé virtuel (VPN).

5 Solution

Appliquer le correctif fourni par CheckPoint selon la version affectée (cf. Documentation).

6 Documentation

- Alerte de sécurité CheckPoint du 28 juillet 2004 :
<http://www.checkpoint.com/techsupport/alerts/asn1.html>
- Référence CVE CAN-2004-0699 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0699>

Gestion détaillée du document

29 juillet 2004 version initiale.