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 janvier 2004
N° CERTA-2004-AVI-019

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du filtre H.323 du garde-barrière Firewall-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-019

Gestion du document

Référence	CERTA-2004-AVI-019
Titre	Vulnérabilité du filtre H.323 du garde-barrière Firewall-1
Date de la première version	29 janvier 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité "H.323 Security Vulnerability" de Check Point
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 ;
- déni de service.

2 Systèmes affectés

Check Point Firewall-1.

3 Résumé

Une vulnérabilité présente dans le filtre H.323 du garde-barrière Check Point Firewall-1 peut être exploitée à distance par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

H.323 est un protocole utilisé par les applications de téléphonie sur IP et de visio-conférence.

Une vulnérabilité présente dans le filtre H.323 du garde-barrière Check Point Firewall-1 peut être exploitée à distance par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

Par défaut, le garde-barrière Firewall-1 analyse le trafic H.323.

5 Contournement provisoire

Dans l'attente de l'application du correctif, désactiver le filtre H.323 ou empêcher tout trafic sur les ports 1720/tcp et 1720/udp utilisé par le protocole H.323.

6 Solution

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

7 Documentation

- Bulletin de sécurité "H.323 Security Vulnerability" de Check Point :
  http://www.checkpoint.com/techsupport/alerts/h323.html
- Avis de sécurité 006489/H323 du NISCC :
  http://www.uniras.gov.uk/vuls/2004/006489/h323.htm

Gestion détaillée du document

29 janvier 2004 version initiale.