

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits ZoneAlarm

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-2005-AVI-071>

Gestion du document

Référence	CERTA-2005-AVI-071
Titre	Vulnérabilité dans les produits ZoneAlarm & Check Point Integrity
Date de la première version	14 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Zone Labs du 11 février 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

- ZoneAlarm 5.x ;
- ZoneAlarm Pro 5.x ;
- ZoneAlarm Security Suite 5.x ;
- ZoneAlarm avec Antivirus 5.x ;
- ZoneAlarm Wireless Security 5.x ;
- Check Point Integrity 4.x ;
- Check Point Integrity 5.x.

3 Description

Une vulnérabilité présente dans de nombreux produits ZoneAlarm et Check Point Integrity permet à un utilisateur local mal intentionné d'effectuer un déni de service sur le système vulnérable. Cette vulnérabilité est due à une mauvaise gestion d'un des paramètres fournis à la fonction `NtConnectPort()`.

4 Solution

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

5 Documentation

- Bulletin de sécurité Zone Labs du 11 février 2005 :
<http://download.zonelabs.com/bin/free/securityAlert/19.html>
- Bulletin de sécurité iDEFENSE “ZoneAlarm 5.1 Invalid Pointer Dereference Vulnerability” du 11 février 2005 :
<http://www.odefense.com/application/poi/display?id=199&type=vulnerabilities>
- Référence CVE CAN-2005-0114 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0114>

Gestion détaillée du document

14 février 2005 version initiale.