

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Winpcap

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-2007-AVI-289>

Gestion du document

Référence	CERTA-2007-AVI-289
Titre	Vulnérabilité dans Winpcap
Date de la première version	10 juillet 2007
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 4.0.1 de winpcap
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 ;
- élévation de privilèges.

2 Systèmes affectés

Winpcap version 4.0 et antérieures.

3 Résumé

Une vulnérabilité dans winpcap permet à un utilisateur local malintentionné d'exécuter du code arbitraire et d'élever ses privilèges.

4 Description

Un manque de contrôle dans la mise en œuvre d'un appel système fourni par le pilote NPF.SYS permet à un utilisateur local d'écraser des zones arbitraires de mémoire du noyau et potentiellement d'exécuter du code arbitraire en espace noyau via l'utilisation particulière de cet appel système.

5 Solution

La version 4.0.1 de Winpcap corrige le problème :
<http://www.winpcap.org/install/default.htm>

6 Documentation

- Site de Winpcap :
<http://www.winpcap.org>
- Liste des changements apportés à la version 4.0.1 :
<http://www.winpcap.org/misc/changelog.htm>

Gestion détaillée du document

10 juillet 2007 version initiale.