

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le service DHCP de Microsoft Windows

---

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-393>

---

### Gestion du document

Référence	CERTA-2004-AVI-393
Titre	Vulnérabilité dans le service DHCP de Microsoft Windows
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-042
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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Microsoft Windows NT Server 4.0 SP6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition SP6.

## 3 Résumé

Une vulnérabilité présente dans le service DHCP (Dynamic Host Configuration Protocol) permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

Le protocole DHCP est le protocole qui permet d'allouer dynamiquement une adresse IP sur un réseau local.

Une vulnérabilité sur le service DHCP permet à un utilisateur mal intentionné, via l'envoi d'un message DHCP malicieusement construit vers un serveur DHCP, de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur le système vulnérable.

Le service DHCP n'est pas activé par défaut sur les systèmes vulnérables.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Microsoft MS04-042 du 14 décembre 2004 :  
<http://www.microsoft.com/technet/security/bulletin/MS04-042.mspx>
- Référence CVE CAN-2004-0899 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0899>
- Référence CVE CAN-2004-0900 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0900>

## **Gestion détaillée du document**

**15 décembre 2004** version initiale.