

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Winsock Hostname et le Client DNS 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-2006-AVI-339>

---

### Gestion du document

Référence	CERTA-2006-AVI-339
Titre	Vulnérabilités dans Winsock Hostname et le Client DNS de Microsoft Windows
Date de la première version	09 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-041 du 08 août 2006
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.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 (Service Pack 1 inclus) ;
- Microsoft Windows Server 2003 x64 Edition et Itanium Edition.

## 3 Résumé

Deux vulnérabilités ont été identifiées dans le système d'exploitation Microsoft Windows, impliquant la fonction `Winsock Hostname` et le client DNS. Une personne malveillante pourrait exploiter l'une d'elles afin d'exécuter du code arbitraire à distance, et prendre le contrôle intégral de la machine vulnérable.

## 4 Description

Deux vulnérabilités, de type débordement de mémoire tampon, ont été identifiées dans le système d'exploitation Microsoft Windows, impliquant la fonction `Winsock Hostname` et le client DNS (pour `Domain Name System`). Celles-ci sont chargées de la résolution de noms, c'est-à-dire la gestion des noms de machines associées aux adresses IP. `Winsock Hostname` est une interface API procurant la fonction d'accès au protocole réseau DNS. Cette interface est utilisée par la majorité des applications nécessitant un accès réseau. Le client DNS est, quant à lui, nativement installé sur la plupart des machines pour effectuer la résolution de noms. Les deux partagent plusieurs fonctions en commun, comme `gethostbyname()`.

Une personne maveillante peut exploiter à distance l'une de ces vulnérabilités pour exécuter du code arbitraire et prendre le contrôle de la machine vulnérable.

## 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 MS06-041 du 08 août 2006 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-041.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-041.msp>
- Référence CVE CVE-2006-3440 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3440>
- Référence CVE CVE-2006-3441 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3441>

## Gestion détaillée du document

09 août 2006 version initiale.