

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service WINS de Microsoft

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-384>

Gestion du document

Référence	CERTA-2004-AVI-384-001
Titre	Vulnérabilité du service WINS de Microsoft
Date de la première version	02 décembre 2004
Date de la dernière version	15 décembre 2004
Source(s)	Bulletin de sécurité Microsoft MS04-045 Bulletin de sécurité US-CERT VU#145134
Pièce(s) jointe(s)	

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 Server, Advanced Server & Datacenter Server ;
- Microsoft Windows NT 4.0 Server & Terminal Server Edition ;
- Microsoft Windows Server 2003 Web Edition, Standard Edition, Enterprise Edition & Datacenter Edition.

3 Résumé

Une vulnérabilité présente dans le service WINS de Microsoft permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Le service WINS (Windows Internet Name Server) de Microsoft permet de traduire le nom NetBIOS d'une machine Windows en adresse IP, et inversement. La fonction appelée WINS Replication qui permet le partage d'informations entre serveurs WINS présente une vulnérabilité dans le traitement des paquets reçus. Cette vulnérabilité permet à un utilisateur d'exécuter du code arbitraire à distance au moyen d'un paquet malicieusement constitué.

5 Contournement provisoire

- Filtrer le port 42 (TCP & UDP) au niveau du pare-feu ;
- sécuriser les communications entre les serveurs WINS au moyen d'IPSec ;
- dans la mesure du possible, ne pas utiliser le service WINS.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft MS04-045 :
<http://www.microsoft.com/technet/security/bulletin/MS04-045.msp>
- Bulletin de sécurité d'IMMUNITY publié le 26 novembre 2004 :
<http://www.immunitysec.com/downloads/instantanea.pdf>
- Bulletin de sécurité US-CERT VU#145134 :
<http://www.kb.cert.org/vuls/id/145134>

Gestion détaillée du document

02 décembre 2004 version initiale.

15 décembre 2004 Ajout du bulletin de sécurité Microsoft et de la section *Solution*.