

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service Microsoft WINS

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-2008-AVI-305>

Gestion du document

Référence	CERTA-2008-AVI-305
Titre	Vulnérabilité du service Microsoft WINS
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-034 du 10 juin 2008
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

- Windows 2000 Server Service Pack 4 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 (SP1 et SP2) pour systèmes Itanium.

3 Résumé

Une vulnérabilité a été identifiée dans le service Microsoft de résolution de noms WINS (*Windows Internet Naming Service*). Elle peut être exploitée par une personne ayant accès au réseau local via une trame spécialement construite afin de prendre le contrôle du système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans le service Microsoft de résolution de noms WINS (*Windows Internet Naming Service*). Les structures de données insérées dans certaines trames ne seraient pas correctement interprétées.

Cette vulnérabilité peut être exploitée par une personne ayant accès au réseau local via une trame spécialement construite afin de prendre le contrôle du système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-034 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-034 du 10 juin 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-034.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-034.msp>
- Référence CVE CVE-2008-1451 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1451>

Gestion détaillée du document

11 juin 2008 version initiale.