

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans les serveurs Windows DNS et 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-2009-AVI-093>

---

### Gestion du document

Référence	CERTA-2009-AVI-093
Titre	Vulnérabilités dans les serveurs Windows DNS et WINS
Date de la première version	10 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-008 du 10 mars 2009
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Les serveurs DNS et WINS pour les versions suivantes :

- Microsoft Windows 2000 Server Service Pack 4 ;
- Windows 2003 Server Service Pack 1 et Service Pack 2 ;
- Windows 2003 Server Edition x64 (Service Pack 2 compris) ;
- Windows 2003 Server pour systèmes basés sur Itanium (Service Pack 1 et Service Pack 2) ;
- Windows 2008 Server pour les systèmes 32-bit ou x64.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les serveurs DNS et WINS de Microsoft Windows. L'exploitation de ces vulnérabilités permet à une personne malveillante distante, par le biais de trames spécialement construites, de détourner du trafic légitime.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans les serveurs DNS et WINS de Microsoft Windows :

- le serveur ne valide pas correctement certaines requêtes en s'appuyant sur les informations mises en cache. Cette vulnérabilité permet à une personne malveillante, par le biais de trames spécialement construites, de corrompre des données en cache. Cette attaque est semblable à celle présentée l'an dernier dans le bulletin d'actualité CERTA-2008-ACT-028 ;
- le serveur ne traite pas correctement certaines réponses DNS erronées, ce qui peut également conduire à un empoisonnement des données mises en cache ;
- le serveur ne valide pas correctement les enregistrements de type WPAD (*Web Proxy Auto-Discovery*) (et ISATAP pour les tunnels IPv6).

## 5 Solution

Se référer au bulletin de sécurité MS09-008 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS09-008 du 10 mars 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-008.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp>
- Référence CVE CVE-2009-0093 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0093>
- Référence CVE CVE-2009-0094 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0094>
- Référence CVE CVE-2009-0233 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0233>
- Référence CVE CVE-2009-0234 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0234>

## Gestion détaillée du document

**10 mars 2009** version initiale.