



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 14 septembre 2011
N° CERTA-2011-AVI-510

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2011-AVI-510>

Gestion du document

Référence	CERTA-2011-AVI-510
Titre	Vulnérabilité dans Microsoft WINS
Date de la première version	14 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-070 du 13 septembre 2011
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

Élévation de privilèges.

2 Systèmes affectés

- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 for Itanium-based Systems ;
- Windows Server 2008 for 32-bit Systems Service Pack 2 ;
- Windows Server 2008 for x64-based Systems Service Pack 2 ;
- Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1.

3 Résumé

Une vulnérabilité dans Microsoft WINS (*Windows Internet Name Service*) permet à une personne malintentionnée d'élever ses privilèges.

4 Description

Une vulnérabilité dans Microsoft WINS permet à une personne munie d'un compte local d'élever ses privilèges sur le système vulnérable via la réception de paquets de réplication WINS spécialement conçu.

5 Solution

Se référer au bulletin de sécurité Microsoft MS11-070 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS11-070 du 13 septembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-070>
<http://www.microsoft.com/technet/security/Bulletin/MS11-070.mspx>
- Référence CVE CVE-2011-1984 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1984>

Gestion détaillée du document

14 septembre 2011 version initiale.