

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service MSMQ 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-2009-AVI-328>

Gestion du document

Référence	CERTA-2009-AVI-328
Titre	Vulnérabilité dans le service MSMQ Microsoft Windows
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-040 du 11 août 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 ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista ;
- Windows Vista Édition x64.

3 Résumé

Une vulnérabilité a été identifiée dans le service de mise en file d'attente MSMQ de Microsoft Windows. Un utilisateur local peut chercher à l'exploiter pour élever ses privilèges.

4 Description

Une vulnérabilité a été identifiée dans le service de mise en file d'attente MSMQ de Microsoft Windows. Le service vérifie de façon incorrecte les données en entrée avant de les transmettre au tampon. Le service n'est cependant pas activé par défaut. Dans le cas contraire, une personne peut chercher à exploiter cette vulnérabilité afin d'élever ses privilèges locaux.

5 Solution

Se référer au bulletin de sécurité MS09-040 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-040 du 11 août 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-040.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-040.msp>
- Référence CVE CVE-2009-1922 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1922>

Gestion détaillée du document

12 août 2009 version initiale.