

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service Message Queuing de 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-2007-AVI-536>

Gestion du document

Référence	CERTA-2007-AVI-536
Titre	Vulnérabilité dans le service Message Queuing de Microsoft Windows
Date de la première version	12 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-065 du 11 décembre 2007
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

- Microsoft 2000 et 2000 Pro service pack 4 ;
- Microsoft XP service pack 2.

3 Résumé

Une vulnérabilité a été découverte dans le service Message Queuing de Microsoft Windows. Cette vulnérabilité permet d'exécuter du code arbitraire à distance ou d'élérer ses privilèges.

4 Description

Une vulnérabilité a été découverte dans le service MSMQ (Microsoft Message Queuing). Cette vulnérabilité est due à une mauvaise gestion des chaînes de caractères transmises au service. Elle peut être exploitée par un

utilisateur mal intentionné afin d'exécuter des commandes arbitraires à distance ou d'élever ses privilèges suivant la version du système d'exploitation vulnérable, via un message MSMQ spécifiquement construit.

Ce service (MSMQ) n'est pas installé en standard pour les systèmes affectés.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS07-065 du 11 décembre 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-065.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-065.msp>
- Référence CVE CVE-2007-3039 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3039>

Gestion détaillée du document

12 décembre 2007 version initiale.