Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2009
N° CERTA-2009-AVI-329

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le Service Station de Travail 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-329

Gestion du document

Référence	CERTA-2009-AVI-329
Titre	Vulnérabilité dans le Service Station de Travail Microsoft Windows
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-041 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

- Windows XP Service Pack 2 et Windows XP Service Pack 3 ;
- 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 Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista Édition x64, Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2.

3 Résumé

Une vulnérabilité a été identifiée dans le Service Station de Travail de Microsoft Windows. Celle-ci peut être exploitée par une personne distante ou locale afin d'élever ses privilèges.

4 Description

Une vulnérabilité a été identifiée dans le Service Station de Travail de Microsoft Windows. Celui-ci alloue et libère la mémoire de manière incorrecte lors de la réception de messages RPC spécialement conçus. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait exécuter du code arbitraire avec des privilèges élevés.

5 Solution

Se référer au bulletin de sécurité MS09-041 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-041 du 11 août 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-041.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-041.mspx
- Référence CVE CVE-2009-1544 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1544

Gestion détaillée du document

12 août 2009 version initiale.