Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 avril 2007
N° CERTA-2007-AVI-168

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de CSRSS dans Microsoft Windows

Gestion du document

Référence	CERTA-2007-AVI-168
Titre	Multiples vulnérabilités de CSRSS dans Microsoft Windows
Date de la première version	11 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-021 du 10 avril 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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 compris).
- Microsoft Windows Server 2003 (Service Pack 1 et Service Pack 2 inclus) ;
- Microsoft Windows Server 2003 pour les systèmes Itanium (Service Pack 1 et Service Pack 2 inclus) ;
- Microsoft Windows Server 2003 x64 Edition (Service Pack 2 inclus) ;
- Windows Vista ;
- Windows Vista x64 Edition.

3 Résumé

De multiples vulnérabilités ont été identifiées dans le processus *Client/Server Runtime Subsystem* ou `CSRSS` de Microsoft Windows. L'exploitation de celles-ci permettraient à une personne malveillante de perturber ou prendre le contrôle complet du système vulnérable.

4 Description

De multiples vulnérabilités ont été identifiées dans le processus *Client/Server Runtime Subsystem* ou `CSRSS` de Microsoft Windows. Ce dernier est un élément essentiel du système d'exploitation, qui permet entre autres de gérer les fenêtres et des éléments graphiques de Windows.

- `csrss.exe` ne manipulerait pas correctement certains messages d'erreurs via ses fenêtres `MsgBox`. Une personne malveillante pourrait donc forcer l'affichage de tels messages particuliers (visite d'une page Web, ou lancement d'une application) afin de prendre le contrôle du système vulnérable ;
- `csrss.exe` ne convertirait pas correctement certaines ressources système, ce qui pourrait également être exploité pour prendre le contrôle d'un système ;

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 MS07-021 du 11 avril 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-021.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-021.mspx
- Bulletin de sécurité eEye AD20070410b du 10 avril 2007 :
  http://www.eeye.com/html/research/advisories/published/AD20070410b.html
- Référence CVE CVE-2006-6696 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6696
- Référence CVE CVE-2006-6797 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6797
- Référence CVE CVE-2007-1209 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1209

Gestion détaillée du document

11 avril 2007 version initiale.