



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 janvier 2012  
N° CERTA-2012-AVI-009

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le processus CSRSS de 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-2012-AVI-009>

---

### Gestion du document

Référence	CERTA-2012-AVI-009
Titre	Vulnérabilité dans le processus CSRSS de Windows
Date de la première version	11 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-003 du 10 janvier 2012
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 XP Service Pack 3 ;
- Windows XP Professionnel x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 pour les systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista Edition x64 Service Pack 2 ;
- Windows Server 2008 Service Pack 2 ;
- Windows Server 2008 Service Pack 2 pour systèmes 64 bits ;
- Windows Server 2008 Service Pack 2 pour systèmes Itanium.

### 3 Résumé

Une vulnérabilité dans le processus CSRSS (*Windows Client/Server Run-time Subsystem*) permet à une personne malintentionnée d'élever ses privilèges.

### 4 Description

Une vulnérabilité présente dans le processus CSRSS (*Windows Client/Server Run-time Subsystem*) permet à un attaquant d'élever ses privilèges s'il est capable de se connecter au système et d'exécuter une application spécialement conçue. L'attaquant pourrait alors prendre le contrôle total du système.

Cette vulnérabilité ne peut être exploitée que sur les systèmes dont les paramètres régionaux sont définis sur chinois, japonais ou coréen. Elle réside dans la façon dont le processus CSRSS traite une séquence de caractères Unicode.

### 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 MS12-003 du 10 janvier 2012 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-003>  
<http://technet.microsoft.com/en-us/security/bulletin/MS12-003>
- Référence CVE CVE-2012-0005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0005>

### Gestion détaillée du document

11 janvier 2012 version initiale.