



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 décembre 2011  
N° CERTA-2011-AVI-694

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2011-AVI-694>

---

### Gestion du document

Référence	CERTA-2011-AVI-694
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	14 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-097 du 13 décembre 2011
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

- Microsoft Windows XP SP3 ;
- Microsoft Windows XP Pro SP2 (64 bits) ;
- Microsoft Windows Vista SP2 (32 bits et 64 bits) ;
- Microsoft Windows 7 SP1 (32 bits et 64 bits) ;
- Microsoft Windows Server 2003 SP2 (32 bits, 64 bits et Itanium) ;
- Microsoft Windows Server 2008 SP2 (32 bits, 64 bits et Itanium) ;
- Microsoft Windows Server 2008 R2 (64 bits et Itanium) ;
- Microsoft Windows Server 2008 R2 SP1 (64 bits et Itanium).

## 3 Résumé

Une vulnérabilité a été corrigée dans Microsoft Windows et permet à un utilisateur malintentionné d'élever ses privilèges sur le système.

## 4 Description

Une vulnérabilité dans le processus CSRSS (*Client-Server Run-time Subsystem*) a été corrigée. Elle permet à un utilisateur malintentionné, disposant d'un accès au système, d'élever ses privilèges en utilisant une application spécialement conçue.

## 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 MS11-097 du 13 décembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-097>  
<http://technet.microsoft.com/en-us/security/bulletin/MS11-097>
- Référence CVE CVE-2011-3408 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3408>

## Gestion détaillée du document

14 décembre 2011 version initiale.