

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans le sous-système win32k 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-2011-AVI-554>

---

### Gestion du document

Référence	CERTA-2011-AVI-554
Titre	Multiples vulnérabilités dans le sous-système win32k de Microsoft Windows
Date de la première version	12 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS-11-077 du 11 Octobre 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

- Exécution de code arbitraire à distance ;
- déni de service ;
- élévation de privilèges.

## 2 Systèmes affectés

Toutes les versions de Windows.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans le sous-système win32k de Windows, dont certaines permettent l'exécution de code arbitraire à distance.

## 4 Description

Ces vulnérabilités permettent, entre autre, d'élever ses privilèges ou d'exécuter du code arbitraire à distance via l'ouverture d'un fichier de polices de caractères spécialement conçu.

## 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 MS11-077 du 11 octobre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/ms11-077>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-077.msp>
- Référence CVE CVE-2011-1985 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1985>
- Référence CVE CVE-2011-2002 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2002>
- Référence CVE CVE-2011-2003 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2003>
- Référence CVE CVE-2011-2011 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2011>

## Gestion détaillée du document

12 octobre 2011 version initiale.