

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la gestion des polices TrueType sur 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-684>

---

### Gestion du document

Référence	CERTA-2011-AVI-684
Titre	Vulnérabilité dans la gestion des polices TrueType sur Windows
Date de la première version	14 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-087 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

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

## 2 Systèmes affectés

Toutes les versions supportées de Microsoft Windows.

## 3 Résumé

Une vulnérabilité dans la gestion des polices TrueType de Windows permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité présente dans le noyau de Windows permet d'exécuter du code arbitraire à distance et d'élever ses privilèges au niveau système. Elle est déclenchée lors de l'ouverture par l'utilisateur d'un document contenant une police de caractères TrueType spécialement conçue.

Cette vulnérabilité a été détaillée dans l'alerte du CERTA CERTA-2011-ALE-006.

## **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 MS11-087 du 13 décembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-087>  
<http://technet.microsoft.com/en-us/security/bulletin/MS11-087>
- Alerte du CERTA CERTA-2011-ALE-006 du 04 novembre 2011 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-006>
- Avis de sécurité Microsoft 2639658 du 03 novembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/advisory/2639658>  
<http://technet.microsoft.com/en-us/security/advisory/2639658>
- Référence CVE CVE-2011-3402 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402>

## **Gestion détaillée du document**

**14 décembre 2011** version initiale.