

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le pilote Compact Font Format (CFF) OpenType

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-062>

Gestion du document

Référence	CERTA-2011-AVI-062
Titre	Vulnérabilité dans le pilote Compact Font Format (CFF) OpenType
Date de la première version	09 février 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-007 du 08 Février 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

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

3 Résumé

Une vulnérabilité a été corrigée dans le pilote Compact Font Format (CFF) OpenType. Elle permet à un utilisateur malintentionné d'élever ses privilèges ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été corrigée dans le pilote Compact Font Format (CFF) OpenType. Elle permet à un utilisateur malintentionné d'élever ses privilèges (Windows XP et Server 2003) ou d'exécuter du code arbitraire à distance (autres versions de Windows) au moyen d'une police CFF spécialement conçue et en incitant sa visualisation par un utilisateur.

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 MS11-007 du 08 février 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-007.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-007.msp>
- Référence CVE CVE-2011-0033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0033>

Gestion détaillée du document

09 février 2011 version initiale.