Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 décembre 2010
N° CERTA-2010-AVI-595

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le pilote de police OpenType

Gestion du document

Référence	CERTA-2010-AVI-595
Titre	Vulnérabilités dans le pilote de police OpenType
Date de la première version	15 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-091 du 14 décembre 2010
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 x64 SP2 ;
- Windows Server 2003 SP2 ;
- Windows Server 2003 x64 SP2 ;
- Windows Server 2003 Itanium SP2 ;
- Windows Vista SP1 et SP2 ;
- Windows Vista x64 SP1 et SP2 ;
- Windows Server 2008 ;
- Windows Server 2008 SP2 ;
- Windows Server 2008 x64 ;
- Windows Server 2008 x64 SP2 ;
- Windows Server 2008 Itanium ;

- Windows Server 2008 Itanium SP2 ;
- Windows 7 32 bits et 64 bits ;
- Windows Server 2008 r2 x64 et Itanium.

3 Résumé

Plusieurs vulnérabilités dans le pilote de police `OpenType` permettent l'exécution de code arbitraire à distance ou une élévation de privilèges.

4 Description

Plusieurs vulnérabilités dans le pilote de police `OpenType` permettent l'exécution de code arbitraire à distance ou une élévation de privilèges. L'attaquant pourrait par exemple héberger une police `OpenType` spécialement conçue sur un partage réseau.

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 MS10-091 du 14 décembre 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-091.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-091.mspx
- Référence CVE CVE-2010-3956 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3956
- Référence CVE CVE-2010-3957 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3957
- Référence CVE CVE-2010-3959 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3959

Gestion détaillée du document

15 décembre 2010 version initiale.