Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mai 2012
N° CERTA-2012-AVI-259

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Office, Windows, .NET et Silverlight

Gestion du document

Référence	CERTA-2012-AVI-259
Titre	Multiples vulnérabilités dans Office, Windows, .NET et Silverlight
Date de la première version	09 mai 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS12-034 du 08 mai 2012
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 à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Office 2003 Service Pack 3 ;
- Microsoft Office 2007 Service Pack 2 ;
- Microsoft Office 2010 (sans Service Pack) ;
- Microsoft Office 2010 Service Pack 1 ;
- Microsoft Silverlight 4 ;
- Microsoft Silverlight 5 ;
- Microsoft Windows XP SP3 ;
- Microsoft Windows Professionnel x64 ;
- Microsoft Windows 2003 Service Pack 2 ;
- Microsoft Windows Vista Service Pack 2 ;
- Microsoft Windows 2008 Serveur Service Pack 2 ;

- Microsoft Windows 7 ;
- Microsoft Windows 2008 Serveur R2.

3 Résumé

Dix vulnérabilités ont été corrigées dans *Microsoft Office, Windows, .NET* et *Silverlight*. Elles concernent :
- deux failles dans la gestion des « TrueType Font » pouvant mener à une exécution de code arbitraire à distance ;
- deux failles dans .NET, une affecte l'allocation de tampons, la deuxième les comparaisons des index. L'une peut causer une exécution de code arbitraire à distance et l'autre un déni de service ;
- deux failles dans le composant GDI+, une affecte l'enregistrement du type dans les images EMF, la deuxième est un débordement de tampon dans le tas, les deux vulnérabilités peuvent mener à une exécution de code arbitraire à distance ;
- une faille de type « double libération » dans Silverlight pouvant mener à une exécution de code arbitraire à distance ;
- une faille dans la gestion des messages en mode noyau pouvant mener à une élévation de privilèges ;
- une faille dans la configuration de clavier pouvant mener à une élévation de privilèges ;
- une faille dans le calcul de la barre de navigation pouvant mener à une élévation de privilèges.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS12-034 du 08 mai 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-034
  http://technet.microsoft.com/en-us/security/bulletin/MS12-034
- Référence CVE CVE-2011-3402 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402
- Référence CVE CVE-2012-0159 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0159
- Référence CVE CVE-2012-0162 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0162
- Référence CVE CVE-2012-0164 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0164
- Référence CVE CVE-2012-0165 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0165
- Référence CVE CVE-2012-0167 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0167
- Référence CVE CVE-2012-0176 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0176
- Référence CVE CVE-2012-0180 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0180
- Référence CVE CVE-2012-0181 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0181
- Référence CVE CVE-2012-1848 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1848

Gestion détaillée du document

09 mai 2012 version initiale.