Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2009
N° CERTA-2009-AVI-324

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de la bibliothèque ATL de Microsoft Windows

Gestion du document

Référence	CERTA-2009-AVI-325
Titre	Vulnérabilités de la bibliothèque ATL de Microsoft Windows
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-037 du 11 août 2009
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.

2 Systèmes affectés

- Windows 2000 SP4 ;
- Windows Windows XP S2, SP3 et Édition Media Center 2005 ;
- Windows XP Professionnel Édition x64 SP2 ;
- Windows Windows Server 2003 SP2, y compris versions pour x64 et Itanium ;
- Windows Vista, Vista SP1 et SP2, y compris versions pour x64 ;
- Windows Server 2008 et 2008 SP2 pour architecturess 32 bits, x64 et Itanium.

3 Résumé

Plusieurs vulnérabilités de la bibliothèque ATL de Windows permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités de la bibliothèque ATL (Active template library) de Windows ont été identifiées :

- la première provient de la lecture sans filtrage de données non sûres ;
- la seconde tire son origine de la copie de données non sûres ;
- la troisième résulte du défaut d'initialisation d'un objet ;
- la quatrième est liée à des erreurs dans certains en-têtes ATL ;
- la cinquième provient d'un défaut de gestion de la mémoire.

Pour chacune de ces vulnérabilités, un utilisateur malveillant peut, par le biais d'une page web malveillante, exécuter du code arbitraire sur un système vulnérable avec les droits de l'utilisateur ;

5 Solution

Se référer au bulletin de sécurité MS09-037 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-037 du 11 août 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-037.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-037.mspx
- Référence CVE CVE-2008-0015 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015
- Référence CVE CVE-2008-0020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0020
- Référence CVE CVE-2009-0901 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0901
- Référence CVE CVE-2009-2493 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493
- Référence CVE CVE-2009-2494 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2494

Gestion détaillée du document

12 août 2009 version initiale.