Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2011
N° CERTA-2011-AVI-442

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les contrôles Chart ASP.NET de Microsoft

Gestion du document

Référence	CERTA-2011-AVI-442
Titre	Vulnérabilité dans les contrôles Chart ASP.NET de Microsoft
Date de la première version	10 août 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS-11-066 du 09 août 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

Atteinte à la confidentialité des données.

2 Systèmes affectés

Seule la version 4 de *Microsoft .NET Framework* est concernée sur les systèmes suivants:
- Windows XP Service Pack 3 ;
- Windows XP Professional Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits ;
- Windows 7 pour systèmes 32 bits Service Pack 1 ;

- Windows 7 pour systèmes x64 ;
- Windows 7 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Une vulnérabilité permettant à une personne malintentionnée d'obtenir des informations sensibles a été découverte dans les contrôles Chart *ASP.NET* de *Microsoft*.

4 Description

Une vulnérabilité est présente dans la manière dont les contrôles Chart *ASP.NET* de *Microsoft* traitent certaines URI contenant des caractères spéciaux. Une exploitation réussie de cette vulnérabilité permet à un attaquant de lire le contenu des fichiers présents dans les répertoires et sous-répertoires du site Web vulnérable.

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 MS11-066 du 09 août 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-066.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-066.mspx
- Référence CVE CVE-2011-1977 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1977

Gestion détaillée du document

10 août 2011 version initiale.