

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft .NET

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-2010-AVI-487>

Gestion du document

Référence	CERTA-2010-AVI-487
Titre	Vulnérabilité dans Microsoft .NET
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-077 du 12 octobre 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.

2 Systèmes affectés

- Microsoft .NET Framework 4.0 sur Windows Server 2003 x64 Service Pack 2 ;
- Microsoft .NET Framework 4.0 sur Windows Server 2003 Itanium avec SP2 ;
- Microsoft .NET Framework 4.0 sur Windows Vista x64 Service Pack 1 et Windows Vista x64 Service Pack 2 ;
- Microsoft .NET Framework 4.0 sur Windows Server 2008 x64 et Windows Server 2008 x64 Service Pack 2 ;
- Microsoft .NET Framework 4.0 sur Windows Server 2008 Itanium et Windows Server 2008 Itanium Service Pack 2 ;
- Microsoft .NET Framework 4.0 sur Windows 7 x64 ;
- Microsoft .NET Framework 4.0 sur Windows Server 2008 R2 x64 ;
- Microsoft .NET Framework 4.0 sur Windows Server 2008 R2 Itanium.

3 Résumé

Une vulnérabilité dans Microsoft .NET permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité dans Microsoft .NET peut être exploitée pour exécuter du code arbitraire à distance par le biais d'une page Web spécialement conçue, en utilisant notamment XBAP (XAML Browser Applications).

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 MS10-077 du 12 octobre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-077.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-077.aspx>
- Référence CVE CVE-2010-3228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3228>

Gestion détaillée du document

13 octobre 2010 version initiale.