

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft .NET Framework

---

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-2007-AVI-295>

---

### Gestion du document

Référence	CERTA-2007-AVI-295
Titre	Vulnérabilités dans Microsoft .NET Framework
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-040 du 10 juillet 2007
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 1.0 ;
- Microsoft .NET Framework 1.1 ;
- Microsoft .NET Framework 2.0.

Microsoft .NET Framework 3.0 ne serait pas affecté par ces vulnérabilités.

## 3 Description

Trois vulnérabilités ont été identifiées dans le composant logiciel Microsoft .NET Framework. Ce dernier est souvent installé pour permettre le développement ou l'exécution d'applications tiers.

Le service PE Loader ne vérifierait pas correctement un tampon. Cette vulnérabilité peut être exploitée par un utilisateur local ou distant, afin d'élever ses privilèges et exécuter du code arbitraire sur le système vulnérable.

Les outils d'ASP.NET ne valideraient pas proprement les adresses réticulaires (URL) fournies en entrée. Une personne malveillante pourrait dans certaines conditions exploiter cette vulnérabilité pour obtenir un accès illégitime sur un site Web utilisant ces outils.

Le service `Just In Time (JIT) Compiler` ne vérifierait pas correctement un tampon. Une personne malveillante pourrait exploiter cette vulnérabilité en construisant une page Web particulière et en incitant l'utilisateur à la visiter (par un lien dans un courrier électronique par exemple).

## 4 Solution

Se référer au bulletin de sécurité MS07-040 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Bulletin de sécurité Microsoft MS07-040 du 11 juillet 2007 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-040.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-040.msp>
- Référence CVE CVE-2007-0041 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0041>
- Référence CVE CVE-2007-0042 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0042>
- Référence CVE CVE-2007-0043 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0043>

## Gestion détaillée du document

**11 juillet 2007** version initiale.