



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 décembre 2011  
N° CERTA-2011-AVI-687

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft Time

---

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-2011-AVI-687>

---

### Gestion du document

Référence	CERTA-2011-AVI-687
Titre	Vulnérabilité dans Microsoft Time
Date de la première version	14 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS11-090 du 13 décembre 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professionnel 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 64 bits 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 dans *Microsoft Time* permet l'exécution de code arbitraire à distance.

### 4 Description

Une vulnérabilité a été découverte dans *Microsoft Time*. Un attaquant peut, par le biais d'une page Web spécifique, provoquer l'exécution de code arbitraire à distance. La vulnérabilité n'est pas corrigée par *Microsoft*, mais un contournement est mis en place au moyen d'un *kill bit*. D'autres *kill bits* sont mis à jour par le correctif de *Microsoft*.

### 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 MS11-090 du 13 décembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-090>  
<http://technet.microsoft.com/en-us/security/bulletin/MS11-090>
- Référence CVE CVE-2011-3397 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3397>

## Gestion détaillée du document

14 décembre 2011 version initiale.