



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 octobre 2006  
N° CERTA-2006-AVI-441

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft XML Core Services

---

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-2006-AVI-441>

---

### Gestion du document

Référence	CERTA-2006-AVI-441
Titre	Vulnérabilités dans Microsoft XML Core Services
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-061 du 10 octobre 2006
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

1. Microsoft XML Parser 2.6 (toutes versions) et Microsoft XML Core Services 3.0 (toutes versions) sur :
  - Microsoft Windows 2000 Service Pack 4 ;
  - Microsoft Windows XP Service Pack 1 ;
  - Microsoft Windows XP Service Pack 2 ;
  - Microsoft Windows XP Professional x64 Edition ;
  - Microsoft Windows Server 2003 ;
  - Microsoft Windows Server 2003 Service Pack 1 ;
  - Microsoft Windows Server 2003 et Windows Server 2003 Service Pack 1 pour système Itanium.
2. Microsoft XML Core Services 4.0 sur :
  - Microsoft Windows 2000 Service Pack 4 ;
  - Microsoft Windows XP Service Pack 1 ;

- Microsoft Windows XP Service Pack 2 ;
  - Microsoft Windows Server 2003 ;
  - Microsoft Windows Server 2003 Service Pack 1.
3. Microsoft XML Core Services 5.0 Service Pack 1 sur :
- Microsoft Office 2003 Service Pack 1 et Service Pack 2.
4. Microsoft XML Core Services 6.0 sur :
- Microsoft Windows 2000 Service Pack 4 ;
  - Microsoft Windows XP Service Pack 1 ;
  - Microsoft Windows XP Service Pack 2 ;
  - Microsoft Windows Server 2003 ;
  - Microsoft Windows Server 2003 Service Pack 1.

### 3 Résumé

Deux vulnérabilités découvertes dans Microsoft XML Core Services permettent à un utilisateur mal intentionné de porter atteinte à la confidentialité des données et/ou d'exécuter du code arbitraire à distance.

### 4 Description

Microsoft XML Core Services permet aux clients de concevoir des applications XML au standard XML 1.0.

- Une vulnérabilité dans Microsoft XML Core Services permet à un individu mal intentionné de porter atteinte à la confidentialité des données notamment en ayant accès aux informations de session (cookies).

extensible Stylesheet Language Transformations (XSLT) permet de manipuler des données au format XML.

- Une vulnérabilité dans XSLT peut être exploitée par une personne malveillante afin d'exécuter du code arbitraire à distance.

Ces vulnérabilités peuvent être exploitées au moyen d'un site web spécialement construit.

### 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 MS06-061 du 10 octobre 2006 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS06-061.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-061.msp>
- Référence CVE CVE-2006-4685 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4685>
- Référence CVE CVE-2006-4686 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4686>

### Gestion détaillée du document

11 octobre 2006 version initiale.