



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 septembre 2011  
N° CERTA-2011-AVI-541

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les protocoles SSL/TLS dans Microsoft Windows

---

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-541>

---

### Gestion du document

Référence	CERTA-2011-AVI-541
Titre	Vulnérabilité dans les protocoles SSL/TLS dans Microsoft Windows
Date de la première version	29 septembre 2011
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft 2588513 du 28 septembre 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

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 for Itanium-based Systems ;
- Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 for 32-bit Systems Service Pack 2 ;
- Windows Server 2008 for x64-based Systems Service Pack 2 ;
- Windows Server 2008 for Itanium-based Systems Service Pack 2 ;
- Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1 ;
- Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1 ;

- Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1 ;
- Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1.

### **3 Résumé**

Une vulnérabilité des protocoles SSL et TLS implémentés dans les logiciels Microsoft Windows peut porter atteinte à la confidentialité des données.

### **4 Description**

Une vulnérabilité dans les protocoles SSL 3.0 et TLS 1.0 permet à un attaquant de déchiffrer les informations acheminées.

### **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

### **6 Documentation**

- Avis de sécurité Microsoft 2588513 du 28 septembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/advisory/2588513>
- Référence CVE CVE-2011-3389 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389>

## **Gestion détaillée du document**

**29 septembre 2011** version initiale.