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 juillet 2012
N° CERTA-2012-AVI-381

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité dans le protocole de chiffrement TLS**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-AVI-381 |
| Titre | Vulnérabilité dans le protocole de chiffrement TLS |
| Date de la première version | 11 juillet 2012 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS12-049 du 10 Juillet 2012 |
| 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 Professionnel Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista Edition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 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 le protocole de chiffrement TLS a été corrigée. Elle permet à une personne malintentionnée de déchiffrer du trafic TLS.

# 4 Solution

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

# 5 Documentation

- Bulletin de sécurité Microsoft MS12-049 du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-049
  http://technet.microsoft.com/en-us/security/bulletin/MS12-049
- Référence CVE CVE-2012-1870 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1870

# Gestion détaillée du document

**11 juillet 2012** version initiale.