



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 août 2010  
N° CERTA-2010-AVI-365

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans SSL/TLS et Secure Channel de 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-2010-AVI-365>

---

### Gestion du document

Référence	CERTA-2010-AVI-365
Titre	Vulnérabilités dans SSL/TLS et Secure Channel de Windows
Date de la première version	11 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-049 du 10 août 2010
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

Windows, toutes versions, toutes éditions.

## 3 Résumé

Deux vulnérabilités affectent le composant Secure Channel de Windows, qui implémente notamment les protocoles TLS et SSL. Leur exploitation permet de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités affectent le composant Secure Channel de Windows :

- (CVE-2009-3555) un problème réside dans les implantation des protocoles TLS et SSL lors de renégociations de sessions. Un utilisateur interposé dans une connexion (*man in the middle*) peut, dans certaines

- circonstances, injecter des données à l'encontre d'un utilisateur et contourner la politique de sécurité ;
- (CVE-2010-2566) une erreur de traitement des certificats de clef publique par Secure Channel sur Windows XP SP3 et Windows Server 2003 (toutes éditions) permet à un utilisateur distant malintentionné d'exécuter du code arbitraire à distance.

## 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 MS10-049 du 10 août 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-049.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-049.msp>
- Document du CERTA CERTA-2009-AVI-482 du 11 août 2010 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-482/index.html>
- Référence CVE CVE-2009-3555 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
- Référence CVE CVE-2010-2566 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2566>

## Gestion détaillée du document

**11 août 2010** version initiale.