



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 22 janvier 2010  
N° CERTA-2010-AVI-025

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Internet Explorer

---

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-025>

---

### Gestion du document

Référence	CERTA-2010-AVI-025
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	22 janvier 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-002 du 21 janvier 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Microsoft Internet Explorer 5.01 ;
- Microsoft Internet Explorer 6.x ;
- Microsoft Internet Explorer 7.x ;
- Microsoft Internet Explorer 8.x.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans Internet Explorer permettent à un utilisateur distant malintentionné de provoquer un déni de service, de contourner la politique de sécurité ou d'exécuter du code arbitraire.

## 4 Description

Une vulnérabilité dans le navigateur Internet Explorer permet de contourner le filtre destinée à empêcher les injections de code indirectes (XSS ou *Cross Site Scripting*). Un utilisateur malveillant peut exploiter cette vulnérabilité pour porter atteinte à la confidentialité des données.

Une vulnérabilité, causée par une erreur dans le traitement des adresses réticulaires (URL), peut être exploitée, au moyen d'une URL spécialement construite afin d'exécuter du code arbitraire à distance.

Plusieurs vulnérabilités dans Internet Explorer permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance au moyen d'une page web spécialement construite.

## 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 MS10-002 du 21 janvier 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-002.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-002.msp>
- Référence CVE CVE-2009-4074 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4074>
- Référence CVE CVE-2010-0027 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027>
- Référence CVE CVE-2010-0244 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0244>
- Référence CVE CVE-2010-0245 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0245>
- Référence CVE CVE-2010-0246 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0246>
- Référence CVE CVE-2010-0247 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0247>
- Référence CVE CVE-2010-0248 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0248>
- Référence CVE CVE-2010-0249 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249>

## Gestion détaillée du document

22 janvier 2010 version initiale.