

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité dans Microsoft 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-ALE-004>

---

### Gestion du document

Référence	CERTA-2010-ALE-004-001
Titre	Vulnérabilité dans Microsoft Internet Explorer
Date de la première version	10 mars 2010
Date de la dernière version	31 mars 2010
Source(s)	Avis de sécurité Microsoft #981374 du 09 mars 2010 Bulletin de sécurité Microsoft MS10-018 du 30 mars 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.

## 2 Systèmes affectés

- Internet Explorer 6 ;
- Internet Explorer 6 Service Pack 1 ;
- Internet Explorer 7.

## 3 Résumé

Une vulnérabilité dans Microsoft Internet Explorer permet l'exécution de code arbitraire à distance. L'éditeur a publié un correctif pour remédier à cette vulnérabilité.

## 4 Description

Une vulnérabilité a été identifiée dans Microsoft Internet Explorer. Son exploitation permet l'exécution de code arbitraire à distance en incitant une victime à visiter une page Web spécialement conçue. L'éditeur Microsoft annonce que plusieurs cas d'attaques utilisant cette faille ont été découverts.

Le CERTA rappelle que si la vulnérabilité touche le navigateur Internet Explorer, d'autres vecteurs que des pages internet peuvent être utilisés. Notamment, il est possible d'exploiter cette faille au moyen de documents Microsoft Office spécialement conçus (cf. bulletin d'actualité CERTA-2009-ACT-012).

## 5 Contournement provisoire

Le CERTA recommande l'application du contournement suivant, qui consiste à retirer les droits d'accès à la bibliothèque `iepeers.dll`. Ceci peut avoir des effets de bord sur certaines fonctionnalités étendues de MSHTML (impression, répertoires Web).

Sur les systèmes 32 bits :

```
Echo y| cacls %WINDIR%\SYSTEM32\iepeers.DLL /E /P "Tout le monde":N
```

Sur les systèmes 64 bits :

```
Echo y| cacls %WINDIR%\SYSWOW64\iepeers.DLL /E /P "Tout le monde":N
```

Pour désactiver ce contournement et autoriser l'accès à cette bibliothèque :

Sur les systèmes 32 bits :

```
cacls %WINDIR%\SYSTEM32\iepeers.dll /E /R "Tout le monde"
```

Sur les systèmes 64 bits :

```
cacls %WINDIR%\SYSWOW64\iepeers.dll /E /R "Tout le monde"
```

Ce contournement fonctionne pour tous les vecteurs d'attaque (page Web, document Microsoft Office, etc.) et est donc recommandé même si Internet Explorer n'est pas le logiciel par défaut utilisé pour la navigation. L'installation d'Internet Explorer 8 permet également de contourner la vulnérabilité pour tous les vecteurs d'attaque.

Si les contournements précédents s'avèrent inapplicables, il est recommandé de naviguer avec un navigateur alternatif et d'appliquer les contournements spécifiques à l'exploitation de la vulnérabilité via des documents Microsoft Office (cf. bulletin d'actualité CERTA-2009-ACT-012).

Le CERTA rappelle, de plus, qu'il recommande de naviguer avec un compte utilisateur aux droits restreints et de désactiver l'interprétation de code dynamique (*Javascript*, *ActiveX*). De plus, l'activation du DEP (*Data Execution Prevention*) peut limiter l'impact de cette vulnérabilité.

## 6 Solution

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

## 7 Documentation

- Bulletin de sécurité Microsoft MS10-018 du 30 mars 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-018.aspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-018.aspx>
- Avis de sécurité Microsoft #981374 du 09 mars 2010 :  
<http://www.microsoft.com/technet/security/advisory/981374.aspx>  
<http://www.microsoft.com/france/technet/security/advisory/981374.aspx>
- Avis du CERTA CERTA-2010-AVI-146 du 31 mars 2010 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-146/>
- Référence CVE CVE-2010-0806 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806>

## Gestion détaillée du document

**10 mars 2010** version initiale.

**31 mars 2010** publication du correctif.