

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité de 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-2005-ALE-017>

---

### Gestion du document

Référence	CERTA-2005-ALE-017-002
Titre	Vulnérabilité de Microsoft Internet Explorer
Date de la première version	21 novembre 2005
Date de la dernière version	14 décembre 2005
Source(s)	Bulletin de sécurité de Computerterrorism CT21-11-2005 du 21 novembre 2005
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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Microsoft Internet Explorer 5.5 ;
- Microsoft Internet Explorer 6.x ;
- Mozilla Suite et Mozilla Firefox (déni de service possible, dépend de la plate-forme).

## 3 Résumé

Une vulnérabilité non corrigée dans Microsoft Internet Explorer permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

## 4 Description

Une vulnérabilité critique non corrigée est présente dans Microsoft Internet Explorer. La vulnérabilité concerne une mauvaise gestion de la fonction Javascript `window()` dans un appel à la fonction `onload`.

Cette vulnérabilité permet à un utilisateur mal intentionné, par l'intermédiaire d'un page malicieusement construite, de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

## 5 Solution

Se référer au bulletin de sécurité Microsoft MS05-054 pour l'obtention du correctif (cf. Documentation).

## 6 Contournement provisoire

- Désactiver le Active Scripting. Pour cela, dans l'onglet Sécurité des options de Microsoft Internet Explorer, cliquer sur le bouton Personnaliser le niveau..., puis dans la section Script et Active Scripting, cocher Désactiver;
- utiliser un navigateur alternatif (voir la section Systèmes affectés pour les navigateurs);
- ne naviguer que sur des sites Internet de confiance.

## 7 Documentation

- Site Internet de Internet Explorer :  
<http://www.microsoft.com/windows/ie/>
- Comment désactiver les contenus actifs sous Internet Explorer :  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;q154036>
- Bulletin de sécurité de Computerterrorism CT21-11-2005 du 21 novembre 2005 :  
<http://www.computerterrorism.com/research/ie/ct21-11-2005>
- Bulletin de sécurité Microsoft #911302 du 21 novembre 2005 :  
<http://www.microsoft.com/technet/security/advisory/911302.msp>
- Bulletin de sécurité de l'US-CERT VU#887861 du 21 novembre 2005 :  
<http://www.kb.cert.org/vuls/id/887861>
- Bulletin de sécurité Microsoft MS05-054 du 13 décembre 2005 :  
<http://www.microsoft.com/france/technet/securite/ms05-054.msp>  
<http://www.microsoft.com/technet/security/Bulletin/ms05-054.msp>
- Bulletin de sécurité du CERTA CERTA-2005-AVI-489 du 14 décembre 2005 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-489/index.html>
- Référence CVE CAN-2005-1790 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790>

## Gestion détaillée du document

**21 novembre 2005** version initiale.

**22 novembre 2005** ajout de la référence au bulletin de sécurité Microsoft, de la référence au bulletin de sécurité US-CERT, précision sur la désactivation de l'Active Scripting et précision sur les navigateurs affectés.

**14 décembre 2005** ajout de la référence au bulletin de sécurité Microsoft MS05-054 et au bulletin de sécurité du CERTA CERTA-2005-AVI-489.